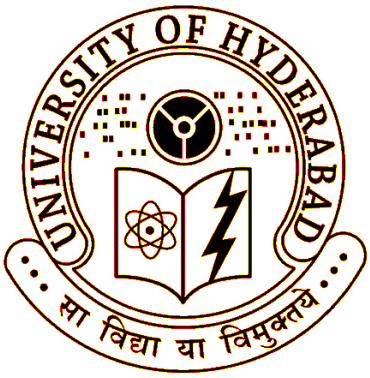
Noise Tolerance and Characterization of Free Space Polarization Shift Keying

A Thesis
Submitted for the Degree of

Doctor of Philosophy



Ram Soorat

School of Physics
University of Hyderabad
Hyderabad-500046
India

2015

Dedicated to

My parents, sir

Declaration

I hereby declare that the work embodied in this thesis entitled "Noise Tolerance and Characterization of Free Space Polarization Shift Keying" is the result of the investigation carried out by me under the guidance of Dr. Ashok Vudayagiri, is a bonafide research work which is also free from plagiarism. I also declare that it has not been submitted to any other University for the award of any degree or diploma. I hereby agree that my thesis can be deposited in Shodganga/INFLIBNET.

Date:
Place: Hyderabad

Ram Soorat

Certificate

This is to certify that Mr. Ram Soorat bearing Regd. No. 08PHPH01, has carried out the research work embodied in the present thesis under my supervision and guidance which is a plagiarism free thesis for a full period prescribed under the Ph.D. ordinance of this University. We recommend his thesis entitled "Noise Tolerance and Characterization of Free Space Polarization Shift Keying" for submission for the award of the degree of Doctor of Philosophy in Physics of this University.

This thesis has not been submitted previously on part or full to this or any other university or institution for the award of any degree or diploma.

Dr. Ashok Vudayagiri
Thesis Supervisor
School of Physics
University of Hyderabad
Hyderabad-500046, India

Dean
School of Physics
University of Hyderabad
Hyderabad-500046, India

Acknowledgment

- I am extremely thankful to my supervisor Dr. Ashok Vudayagiri for giving the opportunity to work in his lab and training me with his scientific knowledge. I express my deepest sense of gratitude for his guidance, constant encouragement, inspiring suggestions and critical discussions throughout my doctoral studies.

- I am thankful to Prof. R. Singh, Dean School of physics and the former Dean Prof. S Chaturvedi, Prof. S.P Tiwari, Prof. C Bansal and Prof. Vipin Srivastva for allowing me to use the department facilities.

- I wish to thank Prof.D. N. Rao, Prof.N. K. Viswanathan, Dr. P. Anantha lakshmi and Dr. Suneel Singh for their guidance during Doctoral Committee meetings. I also thank all the faculty members of the school for all their help and valuable suggestions from time to time. I want to thank the office staff of school of physics especially Mr. Abraham for administrative help.

- I thank Prof. A. K. Kapoor and Dr. E. Harikumar for the most memorable time of my Ph.D. as their teaching assistant.

- I thank all my lab mates and all the MSc project trainees from our lab for making my PhD days memorable.

- I am thankful to my friends and all the research scholars in School of Physics for their timely help and co-operation during my stay in the University.

- I take this opportunity to thank all non teaching staff of School of Physics for their help in all the administrative works.

- I wish to thank Department of information technology (DIT) and Rajiv Gandhi National fellowship (RGNF) for the financial support throughout my doctoral studies.

- I am at a loss of words to express my gratitude to my parents Mr. Shiv Prasad and Mrs. Shubhawati Devi whose teaching since childhood, unending affection and sacrifice has made me achieve this milestone today.

- I wish to thanks Punam for her selfless support.

- I wish to thanks my brother Ram Naresh, sister Anjani and family member Santola Devi, Mahip, Nitish, Anand, Lavkush, Bajrangi, Joginder, Jitender, Pradipika, relatives, and many more for their support and encouragement throughout my doctoral studies.

- My heartfelt thanks to my Quantum optics group members and lab mates for the discussions, criticism and support which made my years in the school an experience that will stay with me forever.

- My time at HCU was made enjoyable in large part due to the friends Rakesh, Abhay, Abhay pratap, Naveen, Suresh, Prateek, Anirudh, Ravi, Sachin, Sanjeev, R.V, Panday, Kishor, Das, shukla, Kapil, krishna, Abhijeet, Madhuri, Suneeta and many more that became a part of my life. I am grateful for time spent with hostel mates and friends.

- Finally, I wish to thank almighty for His / Her blessings which made me stay tuned even after lot of stressful moments during my studies.

Ram Soorat

Contents

1 Introduction **1**

1.1 A brief history of communication 1

1.2 Research motivation and justification 2

1.3 Research objective 4

1.4 Salient features 5

1.5 Thesis organization 6

2 Fundamentals Of Free Space Optical Communication **15**

2.1 Introduction 15

2.2 Features of FSO communications 17

2.3 Areas of application 18

2.4 System configuration 20

2.5 Modulation 20

2.5.1 Direct modulation 21

2.5.2 Indirect modulation 22

2.5.3 Intensity modulation formats 22

2.5.4 Amplitude shift keying 23

2.5.5 On-Off Keying 24

2.5.6 Pules position modulation 26

2.5.7 Phase modulation 27

2.5.8 Polarization modulation 28

2.5.9 Why Polarization shift keying (PolSK)? 28

2.5.10 Advantage 28
2.5.11 Disadvantages 29
2.6 System configuration for PolSK 29
2.6.1 Laser selection 31
2.6.2 VCSEL 31
2.7 Atmospheric turbulence 38
2.7.1 Fog composition 40
2.7.2 Smoke composition 42
2.7.3 Characterization of fog and smoke attenuation theoretical approach 43
2.7.4 Atmospheric transmittance 44
2.8 Receiver 46
2.8.1 Photodiode 46
2.8.2 Avalanche photodiode 47
2.8.3 Geiger-mode avalanche photo-diodes 51
2.8.4 Noise in photo-diodes 51
2.9 Theoretical aspect of experimental system 53
2.9.1 Linear polarized light 53
2.9.2 Circular polarized light 54
2.9.3 Elliptical polarized light 55
2.10 Conclusions 55

3 Noise Tolerance and Characterization 65
3.1 Introduction 65
3.2 Synchronization method 67
3.3 Differential polarization method 69
3.4 The concept behind the scheme 71
3.4.1 Degree of polarization and state of polarization 73
3.4.2 Q factor and BER 77
3.5 Stokes vector and Müller matrix analysis for $0^0$and 90^0 polarization based communication 79

3.6 Results & discusssions 82
3.6.1 Smoke 84
3.6.2 Fog 85
3.6.3 vertical & horizontal polarizations based communication 86
3.7 Conclusions 90

4 Noise Tolerant M-ary Polarization Encoding in Noisy Atmospheric Channel 97
4.1 Introduction 97
4.2 Experimental setup 98
4.2.1 Stokes vector and Müller matrix analysis for $45^0$and 135^0 polarization based communication 99
4.2.2 45° & 135° polarizations based communication 102
4.3 Conclusions 104

5 Random Number Generator 107
5.1 Introduction 107
5.2 Random number generator 110
5.2.1 Practical use of random number 111
5.3 Test for randomness 111
5.3.1 P-value 115
5.4 Generation of random number 116
5.5 Chaos based hardware random number generator 116
5.6 Random number using APD 123
5.7 Random number using LabVIEW 126
5.8 Conclusion 129

6 LabVIEW Programming for PolSK 133
6.1 Introduction 133
6.2 PolSK free space communication based on labVIEW 135
6.2.1 LabVIEW transmitter 137
6.2.2 LabVIEW receiver 140

6.3 Error correction 143
6.4 7,4 Hamming code 144
6.4.1 Implementing Hamming using LabVIEW 147
6.5 Conclusions 152

7 Conclusion & Future work **157**
7.1 Conclusions 157
7.2 Future work: Development of a prototype for free space Quantum Key Distribution(QKD) 158
7.3 BB84 protocol 161
7.4 Ekert Protocol 161
7.4.1 QKD and photon statistics 163
7.5 Experimental setup 165

List of Figures

2.1 Generic diagram of communication setup 20
2.2 Schematic diagram of direct modulation 21
2.3 Schematic diagram of indirect modulation 22
2.4 The binary signal is encoded using rectangular pulse amplitude modulation with polar non-return to zero code 24
2.5 The binary signal is encoded using rectangular pulse amplitude modulation with polar return-to-zero code 25
2.6 Pulse position modulation 26
2.7 Block diagram of experimental setup 30
2.8 VCSEL diode 32
2.9 VCSEL structure 33
2.10 The current-optical power relationship 34
2.11 Schematic diagram setup for current optical power characteristic 34
2.12 The current-optical power relationship of a laser diode using polarization beam splitter 35
2.13 Schematic diagram of experimental setup 36
2.14 Intensity profile based on stokes parameter 37
2.15 Transmission loss in free space 39
2.16 The mechanism of convection fog formation 41
2.17 The mechanism of advection fog formation 42
2.18 Quantum efficiency of various dectectors [66] 48
2.19 Gain vs output [67] 50

2.20 APD module 51
2.21 Linearly polarized light at 45^0 54
2.22 Circularly polarized light 54
2.23 Elliptically polarized light 55

3.1 Experimental setup 67
3.2 Left shows the synchronization sequence of the pulses and right shows the BER as a function of No. of transmitted bit 68
3.3 Bit synchronization with different frequency 68
3.4 Synchronization with clock 69
3.5 Left shows the relationship between various trigger pulses right BER as a function of number of transmitted bit 69
3.6 Scattering of photons through a multiply scattering media . . . 72
3.7 Histograms for photon counts 84
3.8 Distribution of state of polarization 85
3.9 Guassian fits for individual peaks 85
3.10 Correlation between transmitted bits 87
3.11 Experimentally obtained BER 87
3.12 Q factors for 89
3.13 Estimated bit error rates 90
3.14 Estimated Bit Error rates 90

4.1 Schematic diagram of the experimental setup 99
4.2 Constellation diagram for binary and quarternary PolSK 99
4.3 Q factor for 45° (left) 102
4.4 BER for 45° (left) 104

5.1 Circuit diagram 117
5.2 Experimental apparatus for sub-harmonic generation 117
5.3 Analog signal output of the Chaos Clock Generator at different frequencies and corresponding Phase plots 120
5.4 Histogram distribution of 0 and 1 (b) bit correlation 120

5.5 Successive bit correlation . . . 121
5.6 Histogram distribution probable finding pair of 00,01,10,11 . . . 122
5.7 (a)Integrated APD device (b)Phase diagram of random output from APD . . . 123
5.8 Histogram distribution of 0 and 1 (b) bit correlation . . . 124
5.9 Successive bit correlation . . . 124
5.10 Histogram distribution probable finding pair of 00,01,10,11 . . . 125
5.11 Phase plots . . . 126
5.12 Histogram distribution of 0 and 1 (b) bit correlation . . . 127
5.13 Successive bit correlation . . . 128
5.14 Histogram distribution probable finding pair of 00,01,10,11 . . . 128

6.1 Schematic diagram for optical communication protocol . . . 136
6.2 Flow chart diagram for transmitter . . . 138
6.3 Rear panel of transmitter which creates random bits and write to port0 . . . 138
6.4 Rear panel of Alice for receiving authentication protocol . . . 139
6.5 Front panel of transmitter . . . 139
6.6 Flow chart diagram for receiver . . . 140
6.7 Rear panel of receiver . . . 141
6.8 Rear panel of Bob for authentication protocol . . . 142
6.9 Front panel of receiver . . . 143
6.10 Hamming error correction program . . . 147
6.11 Efficiency of Haming code . . . 149
6.12 Bobs Generator matrix . . . 151
6.13 QBER after Hamming as a function of . . . 152

7.1 Comparison of the photon statistics . . . 165
7.2 Experimental Setup . . . 166

Abbreviation

3-D	Three-dimensional
AM	Amplitude modulation
ASK	Amplitude shift keying
PSK	Phase shift keying
BER	Bit error rate
BFSK	Binary frequency shift keying
CDMA	Code division multiple access
PolSK	Polarisation shift keying
DSL	Digital subscriber loop
FSK	Frequency shift keying
FSO	Free-space optical communication
Ge	Germanium
HDTV	High definition television
IF	Intermediate frequency
IM/DD	Intensity modulation/direct detection
InGaAs	Indium gallium arsenide
ISI	Inter-symbol interference
LiNbO3	Lithium Niobate
LO	Local oscillator
LOS	Line-of-sight
LPF	Low pass filter
MPolSk	Multilevel pola risation shift keying
MF	Matched filter

MRC	Maximum ratio combining
MSM	Multiple subcarrier modulation
MZI	Mach-Zehnder interferometer
NASA	National Aeronautics and Space Administration
NRZ-OOK	Non-return-to-zero on-off keying
OBPF	Optical bandpass filter
OFDM	Orthogonal frequency division multiplexing
OOK	On-off keying
P/S	Parallel to serial converter
PLC	Power-line communication
PAM	Pulse amplitude modulation
PAPR	Peak-to-average power ratio
PBC	Polarisation beam combiner
PBS	Polarisation beam splitter
PD	Photodiode
PDF	Probability density function
PFM	Pulse frequency modulation
PLL	Phase locked loop
PM	Phase modulation
PPM	Pulse position modulation
PRBS	Pseudo random binary sequence
PSD	Power spectral density
PSK	Phase shift keying
PSK-SIM	Phase shift keying subcarrier intensity
PAPR	Peak to average power ratio
PWM	Pulse width modulation
QW	Quarter wave retarder
RF	Radio frequency
RHC	Right-hand circular
RMS	Root mean square

Rx	Receiver
RZ-OOK	Return-to-zero on-off keying
SIM	Subcarrier intensity modulation
SNR	Signal-to-noise ratio
SOP	State of polarisation
THz	Terahertz
TL	Transmitting laser
Tx	transmitter
UWB	Ultra-wide band
WDM	Wavelength division multiplexing

Chapter 1

Introduction

1.1 A brief history of communication

Communication is process that a massage, no matter how complex is, conveyed between people over limited distance. Human communication with speech began almost 100,000 years ago. Symbols were adopted about 30,000 years ago[1]. Writing appeared about 5000 years ago. Thousands of year ago smoke signal were used for over distance communication. Optical communications, in various forms, have been used for thousands of years. The Ancient Greeks polished their shields to send signals during battle. In 1830's that electrical telecommunication systems started to appear. While telegraph over wire started around 1830, the first wireless communication was by Alexander Graham Bell. Bell and his assistant Charles Sumner Tainter created and tested a light based Photo-phone between two buildings in 1880[2, 3]. This technology was not successful due to atmospheric turbulence, until the advent of laser and optical fiber technologies. Invention of diode lasers in the 1962's (Robert Hall at GE and Marshall Nathan at IBM) and optical fibers by Charles K. Kao and George Hockham in 1966 revolutionized optical communication.

All though the first fiber very noisy due to the contaminants, their performance was soon made better the fiber optics communication has become norm

of the day. But there are many situation in which fiber based system can not be used. For instance fibers are superfluous for on-chip inter connection, or impossible for satellite to earth communication or for those between two mobile units. such as on-chip connectors where fiber are superfluous or like those between mobile unites or satellite where fiber can not be connected [5]-[6]. Free space optical communication is useful in these cases. FSO applications, in both military and civilian fields in particular the access network, have been reported in the last few years in various parts of the world [7, 8, 9, 10, 11, 12, 13, 14]. The FSO has now emerged as a reliable communication technology with rapid deployment of voice, data, and video within the access networks [15, 16, 17]. Integrated hybrid FSO/fiber systems and wavelength division multiplexing (WDM) based FSO systems can be utilized to increase the link span as well as the transmission capacity[18, 19, 20, 21, 22]. The National Aeronautics and Space Administration (NASA) and the European Space Agency (ESA) have successfully applied FSO technology between satellites with a data rate of 10 Gbps [4].

While free space communication setup cheaper and easier setup, it suffers from two constraints (i) it almost always requires a line of sight setup [5, 23, 24] and (ii) it suffers from atmospheric effect such as fog, smoke and turbulence [25, 26, 27, 28, 29]. Once this was fixed, the fiber optic based communication became the norm of the day. The biggest challenges, such as the atmospheric attenuation and the turbulence and the attainment of 99.999% link availability, still have to be circumvented in order to increase the link range and link availability in terrestrial FSO systems [5, 30, 31].

1.2 Research motivation and justification

FSO has become a promising technology due to easy of establishing temporary links in times of emergency, higher data rates, low cast, small size and limited power consumption [34, 35, 36, 37]. FSO also supports all possible

modulation schemes such asamplitude, frequency, phase or polarization. It may be noteworthy that polarization and frequency modulation are impractical in fiber based system, due to their inherent polarization scrambling and frequency dispersion. Free space, on the other hand is free of these effect.

However, FSO links based within earth's atmosphere suffer from due to fluctuation in the atmosphere. Change in refractive index causes beam walk off and phase fluctuation, while fog, smoke etc cause both attenuation as well as polarization scrambling. Yet polarization turns out be a very robust scheme, that's a differential measurement method we used in this study[38, 39, 40].

In this work, we simulated atmospheric conditions such as fog and smoke in our lab and measured its effect on free space optical system. In particular, we show that a polarization modulation scheme, though undergoes depolarization due to atmosphere, shows a high degree of reliability. We show that the experimental setup is remarkable simple, consisting of two VCSEL, one for each polarization. Two detector at the receiver makes a measurement on both polarization components and a differential measurement provides the state of polarization[40, 41, 42, 43]. We then map the data bits based on the ratio of polarized part to depolarized part, as explained in detail in later sections. This allows a reliable communication even in presence of high degree of depolarization. From these measurements we compute the bit error rate and Q-factor depends on the noise which fits to a stretched exponential. This connection require more detail study.

Moeyaert et. al. have theoretically shown that the error rate in case of a Phase Modulation scheme follow a stretched exponential function [44]. However, in this case the BER is a regular exponential while the Q factors follow a stretched exponential function. This aspect requires further investigation. Random numbers are important requirement for both classical encryption as well as quantum key distribution (QKD). Practical Vernam cipher employs addition of a random series of zero's and ones to the arrange to create cipher text. Since software methods only offer a pseudo random number codes, need for other sources is important. Several attempts were made for random number

generator, which would be used for the entire QKD scheme [45, 46].

- Pseudo Random code of LabVIEW
- Hardware generator built around Kuuselas chaos circuit
- Dark Counts from Avalanche Photo Diode

In all these methods we show the efficiency of random number generator by analyzing their statistics. A complete LabVIEW program for standard requirement of a traditional protocol such as hand shaking, identification and acknowledgment is developed to use for PolSK. A (7,4) Hamming code was developed using the LabVIEW. For error correction it was tested by deliberately causing known rate of bit flip errors on a test data. The data after operating Hamming correction was compared with the original data and the uncorrected bit error rate was obtained. Bobs error rate decreases after Hamming operation. However, the efficiency of correction decreases for higher initial error rates. We further want to extend this setup for free space quantum key distribution (QKD). However the success of QKD protocols depend upon the success of the underlying communication method.

1.3 Research objective

In this thesis we experimentally verify the amount of depolarization noise due to fog and smoke and compare with known theoretical values. There has been several studies involving simulations [38, 47] but very few experimental studies to substantiate these simulations. In addition, we provide a more practical measurement technique for determining the state of polarization of the light, which involves less number of measurements compared to a full Stokes parameter determination. Although this technique is useful only in the limited context of the Polarization modulation communication scheme, it is nevertheless offers easier and speedier measurement. We show that this technique has a significantly higher tolerance for depolarization noise. We

also prepared a labVIEW program that involves a complete protocol including authentication, handshaking and error correction. In addition we have tested a few methods of generation of random numbers which are relevant in area of cryptography.

1.4 Salient features

- The analytical and simulation results for the error performance and fading penalty two state polarization (vertical and horizontal) polarization shift keying (PolSK) systems operating over the turbulent atmosphere across the whole turbulence regimes have been detailed in Chapter Three. The SOP, Q-factor, Optical density and BER expressions of the PolSK-FSO system in a turbulence channel have been derived. The comparison with the actual data that was received after using SoP indicates an almost zero BER for Optical Densities as high as -23 dB.

- Similar study has been done for two state polarization ($\pm$ 45) polarization shift keying (PolSK) systems operating over the turbulent atmosphere across the whole turbulence regimes have been detailed in Chapter Four.

- A complete LabVIEW program for standard requirement of a traditional protocol such as hand shaking, identification and acknowledgment is developed to use for PolSK. A (7,4) Hamming code was developed using the LabVIEW detailed in chapter six.

- Quantum error correction has been done before hamming and after hamming detailed in chapter six.

- Different types of random number generator has been studied and tested by NIST test detailed in chapter five.

1.5 Thesis organization

The central idea of the thesis is to characterization of noise tolerance for polarization based communication. Polarization in free space suffer from depolarization yet we are achieving good signal to noise ration by resorting to measurement technique. Keeping this theme in mind the thesis organized in to six chapter for easy understanding and to maintain uniform flow and connectivity.

Chapter 1. Introduction

This chapter begins with historical background to communication and introduction to optical communication. This chapter ends with thesis organization and original contribution.

Chapter 2. Fundamental of free space optical communication

The main focus of this chapter is to explain basic concepts of related equipment that are part of free space optical communication. We provide a brief overview of different modulation techniques, in particular the PolSK scheme used by us. An overview of the experimental system used by us for PolSK is provided and a detail description of components used, such as VCSEL, Avalanche photodiodes etc. A brief mathematical description of PolSK is also provided here.

Chapter 3. Noise tolerance and noise characterization in PolSK

In this chapter we propose a reliable method of measurement for polarization modulation scheme, which involves a differential measurement of the polarization. This method shows a higher degree of reliability since the information bits 0 and 1 can be mapped to a negative value of SoP and a positive value

of SoP respectively. Unless the polarization is completely scrambled, resulting in an SoP of zero, the information can be mapped properly. Below a large threshold value of scattering densities, both estimated and measured Bit Error Rates are nearly zero. Beyond this threshold value the BER raises in a very sharp manner. The comparison with the actual data that was received after using SoP indicates an almost zero BER for Optical Densities as high as -23 dB.

Chapter 4.Noise tolerant M-ary polarization encoding in noisy atmospheric channel

In this chapter we have presented the effect of fog and smoke on 45°/135° polarization. we have shown that unlike case of V/H polarization of Q-factor shows a stretched exponential dependency for both fog and smoke. BER fits to normal exponential function for both cases. The result shows that the decrease in Q-factor and the increase in BER are much smother than in the case for V/H where in they showed a sharp increase/decrease. In addition the noise threshold ratios for the two schemes are different. This effect is of concern for both m-ary encoding as well as QKD schemes. The different amount of degradation in each basis needs to be accounted for when using m-ary protocols of QKD protocol that uses polarization encoding.

Chapter 5. Random number generator

One area where PolSK is very useful is quantum key distribution (QKD). This is a method which exploits rules of quantum mechanics to send a secure key code, usable in Vernam cipher method. The original protocol of QKD such as BB84 and B92 etc are conceived as polarization encoding methods. One key feature necessary for QKD as well as classical Vernam encryption is a sequence of random bits of 0 and 1 the arrange to create cipher text. Since software methods only offer a pseudo random number codes, need for other sources is

important. We have therefore analyzed a few method of generating random number.

Chapter 6. LabVIEW Programming for PolSK

In this chapter we explain a complete program for standard requirement of a traditional protocol such as hand shaking, identification and acknowledgment. We also created a LabVIEW code for error correction of the data using (7,4) Hamming code. It was tested by deliberately causing known rate of bit flip errors on a test data. The data after operating Hamming correction was compared with the original data and the uncorrected bit error rate was obtained. we found that bit error rate after hamming code correction is much smaller.

Chapter 7. Future work and conclusion

In this chapter we summarize our result and discuss its relevance for QKD. Some more aspect of generate random number using VCSEL itself its considered and its application are discussed.

Bibliography

[1] David Diringer "The Book Before Printing: Ancient, Medieval and Oriental", Courier Dover Publications, 1982

[2] Mary Kay Carson, Alexander Graham Bell "Giving Voice To The World" Sterling Biographies, New York, Sterling Publishing. pp. 7678. ISBN 978-1-4027-3230-0. 2007

[3] Alexander Graham Bell "On the Production and Reproduction of Sound by Light", American Journal of Science, Third Series XX (118), 305324. also published as "Selenium and the Photophone" in Nature, September 1880.

[4] H. Hemmati, "Deep space optical communications," in Deep space communications and navigation series, H. Hemmati, Ed. California: Wiley Interscience; 1 edition, April, 2006

[5] Plank, M. Czaputa, E. Leitgeb, S. S. Muhammad, N. Djaja, B. Hillbrand, P. Mandl, and M. Schonhuber,"Wavelength selection on FSO links", Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP), 2508, 2011

[6] N. H. M. Noor, A. W. Naji, and W. Al-Khateeb, "Theoretical analysis of multiple transmitters/receivers on the performance of free space optics (FSO) link", IEEE International Conference on Space Science and Communication, 2011

[7] R. Mesleh, H. Elgala, and H. Haas, "Optical spatial modulation," IEEE/OSA Journal of Optical Communications and Networking, vol. 3, pp. 234-244, 2011.

[8] S. Hardy, "Free-space optics systems are finding their niches," Lightwave, pp. 33-36, December 2005.

[9] C. P. Colvero, M. C. R. Cordeiro, G. V. d. Faria, and J. P. v. d. Weid, "Experimental comparison between far- and near infrared wavelengths in free space optical systems," Microwave and Optical Technology Letters, vol. 46, pp. 319-323, 20 August 2005.

[10] R. Dennis, L. Mark, G. Ganesh, P. Bruce, and N. Gerald, "Optical wireless propagation: theory vs. experiment," Proceedings of SPIE: Optical Wireless Communications III, vol. 4214, pp. 38-45, 2001.

[11] E. Korevaar, I. I. Kim, and B. McArthur, "Atmospheric propagation characteristics of highest importance to commercial free space optics," Proceeding of SPIE, vol. 4976, pp. 1-12, 2003.

[12] D. Y. Song, J. W. Cho, Y. S. Hurh, J. H. Lim, D. W. Lee, and J. S. Lee, "410 Gb/s terrestrial optical free space transmission over 1.2 km using an EDFA preamplifier with 100 GHz channel spacing," Optical Fiber Communication Conference, 2000, vol. 3, pp. 142-144, 2000.

[13] M. D'Amico, A. Leva, and B. Micheli, "Free-space optics communication systems: first results from a pilot field -trial in the surrounding area of Milan, Italy," IEEE Microwave and Wireless Components Letters, vol. 13, pp. 305-307, August 2003.

[14] Y. Ma, S. C. Saha, A. L. Bernassau, and D. R. S. Cumming, "Terahertz free space communication based on acoustic optical modulation and heterodyne detection," Electronics Letters, vol. 47, pp. 868-870, 2011.

[15] H. Tapse, D. K. Borah, and J. Perez-Ramirez, "Hybrid optical/RF channel performance analysis for Turbo codes," IEEE Transactions on Communications, vol. 59, pp. 1389-1399, 2011.

[16] N. D. Chatzidiamantis and G. K. Karagiannidis, "On the distribution of the sum of gamma-gamma variates and applications in RF and optical wireless communications," IEEE Transactions on Communications, vol. 59, pp. 1298-1308, 2011.

[17] M. Gregory and S. Badri-Hoeher, "Characterization of maritime RF/FSO channel," International Conference on Spa ce Optical Systems and Applications (ICSOS) 2011, pp. 21-27, 2011.

[18] K. Kazaura, K. Omae, T. Suzuki, M. Matsumoto, E. Mutafungwa, T. Murakami, K. Takahashi, H. Matsumoto, K. Wakamori, and Y. Arimoto, "Performance evaluation of next generation free-space optical communication system," IEICE Transaction of Electronics, vol. E90-C, pp. 381-388, February 2007.

[19] K. Wang, A. Nirmalathas, C. Lim, and E. Skafidas, "High speed 412.5Gbps WDM optical wireless communication systems for indoor applications," the National Fiber Optic Engineers Conference Optical Fiber Communication Conference and Exposition 2011, pp. 1-3, 2011.

[20] Z. W. Xu, X. F. Cheng, Y. K. Yeo, L. Y. Zhou, X. Shao, and H. G. Zhang, "1.24-Tb/s hybrid SCM/WDM passive optical networks," pp. 1-3, 2011.

[21] S.-R. Moon, H.-K. Lee, and C.-H. Lee, "Automatic wavelength control method using Rayleigh backscattering for WDM-PON with tunable lasers," Conference on Lasers and Electro-Optics (CLEO) 2011, pp. 1-2, 2011.

[22] M. Sjo din, E. Agrell, P. Johannisson, G. W. Lu, P. A. Andrekson, and M. Karlsson, "Filter optimization for self-homodyne coherent WDM systems using interleaved polarization division multiplexing," Journal of Lightwave Technology, vol. 29, pp. 1219-1226, 2011.

[23] S. A. J. Flörez, "Circular polarization and availability in free space optics (FSO) communication systems", IEEE Latin-American Conference on Communications (LATINCOM 2010), 1, 2010

[24] M. Niu, J. Cheng, and J. F. Holzman, "Diversity reception for coherent free-space optical communications over K-distributed atmospheric turbulence channels", IEEE Wireless Communications and Networking Conference (WCNC), 2010

[25] E. Dadrasnia, S. Ebrahimzadeh, and F. R. M. Adikan, "Influence of short range free space optical atmospheric attenuation in modulated radio signal", The 2nd International Conference on Computer and Automation Engineering (ICCAE), **5**, 569 2010

[26] P. P. Smyth, P. L. Eardley, K. T. Dalton, D. R. Wisely, P. McKee, and D. Wood, "Optical wireless: a prognosis", Proceeding of SPIE, **2601**, 212, 1995

[27] S. A. Zabidi, W. A. Khateeb, M. R. Islam, and A. W. Naji, "Investigating of rain attenuation impact on free space optics propagation in tropical region", 4th International Conference On Mechatronics - 2011

[28] L. C. Andrews, R. L. Phillips, and C. Y. Hopen, "Laser Beam Scintillation with Application", SPIE Press, Washington 2001

[29] A. K. Majumdar, "Free Space Laser Communication Performance in the Atmospheric Channel", J. Opt. Fiber. Commun. Rep. **2**, 345, 2005

[30] W. O. Popoola, "Subcarrier intensity modulated free-space optical communication systems," in School of Computing, Engineering and Information Sciences. vol. Doctor of Philosophy Newcastle: University of Northumbria, September 2009, p. 264.

[31] M. N. Khan and W. G. Cowley, "Signal dependent Gaussian noise model for FSO communications," Australian Communications Theory Workshop 2011, pp. 142-147, 2011.

[32] A. Hashmi, A. Eftekhar, S. Yegnanarayanan, and A. Adibi, "Analysis of optimum adaptive optics systems for hybrid RF-wireless optical communication for maximum efficiency and reliability," 4th International Conference on Emerging Technologies, 2008, pp. 62-67, 18-19 October 2008.

[33] I. Kim, R. Stieger, C. Moursund, J. A. Koontz, M. Barclay, P. Adhikari, J. Schuster, and E. Korevaar, "Wireless optical transmission of fast ethernet, FDDI, ATM, and ESCON protocol data using the TerraLink laser communication system," Optical Engineering, vol. 37, pp. 3143-3155, December 1998.

[34] A. Bekkali, C. B. Naila, K. Kazaura, K. Wakamori, and M. Matsumoto, "Transmission analysis of OFDM-based wireless services over turbulent radioon-FSO links modeled by gamma-gamma distribution," IEEE Photonics Journal, vol. 2, pp. 510-520, 2010.

[35] R. R. Iniguez, S. M. Idrus, and Z. Sun, Optical wireless communications - IR for wireless connectivity. London: Taylor & Francis Group, LLC, 2008.

[36] C. B. Naila, A. Bekkali, K. Wakamori, and M. Matsumoto, "Performance analysis of CDMA-based wireless services transmission over a turbulent RF-on-FSO channel," Journal of Optical Communications and Networking IEEE/OSA, vol. 3, pp. 475-486, 2011.

[37] Z. X. Wang, W. D. Zhong, S. N. Fu, and C. Lin, "Performance comparison of different modulation formats over free-space optical (FSO) turbulence links with space diversity reception technique," IEEE Photonics Journal, vol. 1, pp. 277-285, December 2009.

[38] Ijaz M, Ghassemlooy, Z., Le Minh, H. , Rajbhandari S. , Perez J. , Gholami A. "Bit error rate measurement of free space optical communication links under laboratory-controlled fog conditions", 16th European Conference on Networks and Optical Communications (NOC), 52, 2011

[39] John Zweck, Ivan T. Lima Jr, Yu Sun, Aurenice O. Lima, Curtis R. Menyuk, and Gary M. Carter Modeling Receivers in Optical Communication Systems With Polarization Effects, Optics and Photonics News, **14**, 30, 2003

[40] Ram soorat, Ashok vudayagiri " Noise Characterization in Free Space Polarization Modulation Communication Using Simulated Atmospheric Conditions in Laboratory",International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869,2014.

[41] Wolf E., "Introduction to the Theory of Coherence and Polarization of Light", Cambridge University Press, 2007

[42] J. Grosinger, "Investigation of polarization modulation in optical free space communications through the atmosphere." vol. master: Technical University of Vienna, February 2008, p. 77. space diversity reception technique," IEEE Photonics Journal, vol. 1, pp. 277-285, December 2009.

[43] M. M. Karbassian and H. Ghafouri-Shiraz, "Transceiver architecture for incoherent optical CDMA network based on polarization modulation," Journal of Lightwave Technology, vol. 26, pp. 3820-3828, 15 December 2008.

[44] Moeyaert, V., Mgret, P., Froidure, J. C., Robette, L., & Blondel, M. "Analytical formulation of the error probability of a QPSK transmission impaired by the joint action of gaussian and impulse noise", In Proceedings of the Second IASTED International Conference on Communication Systems and Networks, 2003

[45] T. Kuusela, Random number generation using chaotic circuit J. Nonlinear Sci. 3, 445, 1993

[46] Andrew Rukhin , A Statistical Test Suite for Random and Pseudorandom Number Generators for cryptographic Applications, NIST special publication 800-22, 2010

[47] Shalini Khare and Namrata Sahayam, "Analysis of Free Space Optical Communication System for Different Atmospheric Conditions & Modulation Techniques" Int. J. Mod. Eng. Research, **6**, 4149 - 4152

Chapter 2

Fundamentals Of Free Space Optical Communication

2.1 Introduction

Free-space optical communication (FSO) is an optical communication technology that uses light propagating in free space (wireless). The technology is useful where the physical connections are impractical due to high costs or other considerations. In FSO information encoded in optical radiation of electromagnetic fields. The physics of electromagnetic (EM) is very well studied and Maxwell equations are mostly applied in order to understand the propagation of EM waves in different media [1]. EM waves spectrum is very wide, with wavelengths ranging from 10^{-14} up to 10^{4} m. Different bands of frequency are associated with EM waves and very well defined for the communication purposes as well as other application in health and industry [2]. The spectrum is also divided into two regions

1. The ionizing part of the electromagnetic spectrum that includes ultraviolet rays, gamma-rays and x-rays, whose wavelengths are very short and whose intensities are very high and thus are not feasible for wireless communications.

2. The non-ionizing part that includes radio waves, IR and visible light which are mostly used for wireless communications [3].

In FSO links, the information is transferred between two points through optical radiation propagating over unguided channels. The transported data could be embedded into the intensity, phase, frequency or polarization of the optical carrier. In general, FSO is based on line of sight (LOS) communication where the transmitter and the receiver can directly see one another without any obstructions in between [4, 5, 6]. Currently, many diverse applications of FSO are tailored to offer low and very high speed wireless links effectively. Where ever unlimited bandwidth and faster internet connectivity is required, Free Space Optics (FSO) has emerged as a promising solution because devices have become less expensive, more reliable, more powerful, and partly because the RF spectrum has become overly congested. An FSO system for the outdoor environment is workable over distances of several kilometers as far as it has clear LOS of atmosphere between the source and the destination [7]. It is difficult to intercept of a laser beam. Tapping in the system can easily be detected as the intercept equipment must be placed within the very narrow optical footprint. FSO communication systems developed for voice, video and broadband data communications are used by security organizations such as governments and the military [8, 9].

FSO technology has numerous applications, spanning from very short range (mm range) optical interconnects within integrated circuits for clock distribution, to outdoor intra building links of a few kilometers to inter-satellite links [4, 10, 11, 12, 13]. Outdoor terrestrial FSO systems with a link length of a few kilometers have been applied at multi Gbps data rates [5, 14, 15]. One of the main limitations of FSO technology is its susceptibility to weather. Fog or heavy snow via light scattering, attenuation, and absorption which significantly affect the power budget [6, 11, 13, 16, 17]. The FSO links are also influenced by the sun, which is within the receivers field of view. To attain 99:999 link availability during thick fog is still a challenge in FSO technology.

One solution is to use the hybrid FSO/RF system where an RF link as the back-up at a reduced data rate [13, 16, 18]. FSO can be installed in a shorter time and lower cost compare to laying down fiber optic cable [19].

2.2 Features of FSO communications

In basic terms, FSO involves the transfer of data/information between two points using optical radiation as the carrier signal through unguided channels. The data to be transported could be modulated on the intensity, phase, polarization or frequency of the optical carrier. An FSO link is essentially based on line-of sight (LOS), thus to ensure a successful exchange of information requires that both the transmitter and the receiver directly see one another without any obstruction in their path. The unguided channels could be any, or a combination, of space, sea-water or atmosphere. The emphasis in this work is however on terrestrial FSO as such, the channel of interest is the atmosphere [20].

1. In FSO communication most powerful aspect is tremendous bandwidth available at optical frequency. A wave length of $1\mu m$ corresponds to 3 10^{14} Hz(=300,000 GHz) and therefore a single 16 GHz channel corresponds to only $3.310^{-6}\mu m$ of wavelength spread. Optical communication therefore guarantees an increased information capacity compared to radio frequency based communication systems. This is simply because on the electromagnetic spectrum, the optical carrier frequency, which includes infrared, visible and ultra violet frequencies, is far greater than the radio frequency. The usable frequency bandwidth in RF range is comparatively lower by a factor of 10^5 [2, 11, 12, 20].

2. The optical radiation is known for its extremely narrow beam with typical laser beam of diffraction limited divergence of between 0.01 0.1 mrad. Hence the transmitted power is only concentrated within a very narrow area, thus providing an FSO link with adequate spatial isolation from

its potential interferes. The tight spatial confinement also allows for the laser beams to operate nearly independently, providing virtually unlimited degrees of frequency reuse in many environments and makes data interception by unintended users difficult. Conversely, the narrowness of the beam implies a tighter alignment requirement.

3. Due to the congestion of the RF spectrum, interference from adjacent carriers is a major problem facing wireless RF communication. At present, the optical frequencies are free from all of this.

4. FSO communication is cheaper than that of an RF with a comparable data rate. FSO can deliver the same bandwidth as optical fiber but without the extra cost of right of way and trenching. Unlike wired systems, FSO is a non-fixed recoverable asset. It has light weight and is very compact consumes low power .

5. It requires line of sight and strict alignment as a result of its beam narrowness. It is very easy to install FSO communication system to become fully operational, starting from installation down to link alignment. The key requirement is the establishment of an unimpeded line of sight between the transmitter and the receiver. It can also be taken down and redeployed to another location quite easily.

6. FSO communication fully depend on atmospheric conditions. RF and satellite communication links also experience link outages during heavy rainfall and in stormy weather. These properties of the FSO channel undoubtedly pose the greatest challenge.

2.3 Areas of application

The characteristic features of FSO communication is very attractive for various applications within the access and the metro networks. The point that most end users are within a short distance from the backbone one mile or less

makes FSO very attractive as a data bridge between the backbone and the end-users. Among other emerging areas of application, FSO has been found suitable for use in the following areas:

1. FSO is used to bridge the bandwidth gap that exists between the end-users and the fiber optics backbone. Links ranging from 50 m up to a few km are readily available in the market with data rates covering 1 Mbps to 10 Gbps.

2. Used to provide back-up against loss of data or communication break-down in the event of damage or unavailability of the main optical fiber link.

3. It can be used to back-haul traffic between base stations and switching centers in the 3rd/4th generation (3G/4G) networks, as well as transporting IS-95 code division multiple access (CDMA) signals from macro and micro-cell sites to the base stations.

4. The technology finds application where a temporary link is needed, be it for a conference or ad-hoc connectivity in the event of a collapse of an existing communication network.

5. FSO has found applications in interconnecting campus networks and providing back-up links at Fast-Ethernet or Gigabit-Ethernet speeds.

6. FSO is an attractive data bridge in such instances as across a river, a very busy street, rail tracks or where right of way is not available or too expensive to pursue.

7. In view of the huge bandwidth requirement of high definition cameras and television signals, FSO is increasingly being used in the broadcast industry to transport live signals from high definition cameras in remote locations to a central office.

2.4 System configuration

A typical FSO system consist of three parts. In figure 2.1 shows schematic

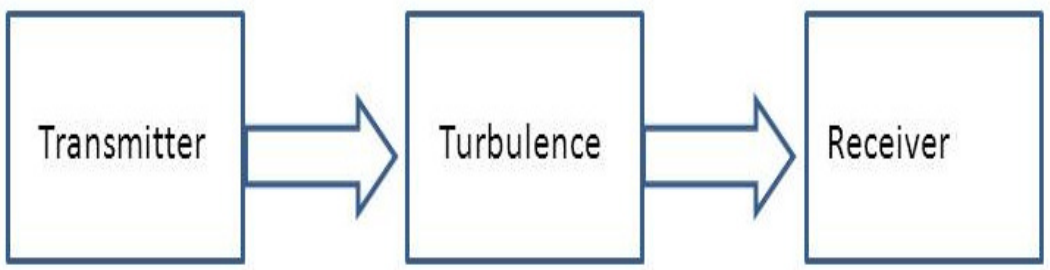


Figure 2.1: Generic diagram of communication setup

diagram of experimental setup for communication its individual component describes in figure 2.7. The transmitter consist of a module where a carrier is modulated. Modulated signals pass through channel with turbulence. Receiver detects it and extracts the information.

2.5 Modulation

In optical communication modulation is the process of conveying a message by using optics. Optical field has three physical attributes (intensity, phase and polarization) which can be used to transmit information. To design an optical wireless system, selecting the right modulation scheme is importance. The bandwidth, the power efficiency and the design complexity of the transmitter and receiver, which affect the overall performance of the system, are defined by the modulation technique adopted [21, 22]. Considering that the atmospheric turbulence mainly affects on the light intensity, pulse-position modulation (PPM) [23, 24, 25, 26] is commonly used in FSO communication. Since fiber-optic technologies have been well developed and fiber-optic networks have been widely deployed from the local access networks to the long-haul intercontinental networks, some commonly used modulation formats in

fiber-optic transmission system, including onoff keying (OOK) [23], and differential phase-shift keying (DPSK) [27], have also been investigated in FSO systems.

2.5.1 Direct modulation

Digital signals consist of logical 1's and 0's, which readily corresponds to electrical ON and OFF states, or to two discrete voltage (or current) levels. The typical optical communications light source is a laser diode, which is easily modulated by controlling its current. Several factors limit the upper frequency at which a laser diode can be modulated. Direct modulation is limited by the characteristics of the diode itself.

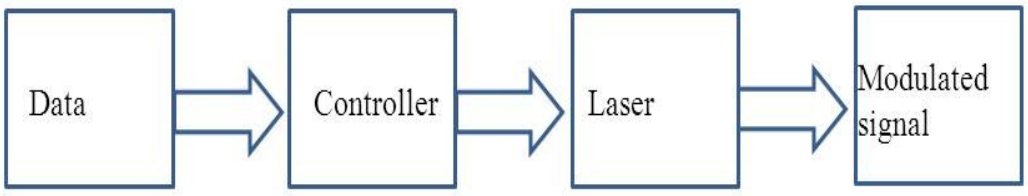


Figure 2.2: Schematic diagram of direct modulation

A full turn-on/turn-off cycle represents a significant electrical and thermal stress, which can result in a frequency shift (chirp), transients (ringing) as well as reduced operational lifetime of the laser diode. One method of dealing with these effects is to apply a modulated radio signal to the diode. The current swing is reduced, which improves reliability, and the bandwidth is greatly increased because the diode's drift and transient responses are reduced. But this technique also greatly reduces the signal-to-noise ratio, which reduces the range, and it requires more complex driver and detector circuitry.

2.5.2 Indirect modulation

Modulation of a continuous light beam removes the laser diode-related problems at the cost of greater complexity. It also eliminates the signal-to-noise problems of applying a modulated sub-carrier. The stable light source allows maximum transmission distance for free space. Established methods include delivering the data to electrically modulated crystalline materials such as lithium niobate. These devices can rapidly switch the light beam between a direct signal path, or split the beam into two paths with 180-degree phase shift, which cancel when recombined.

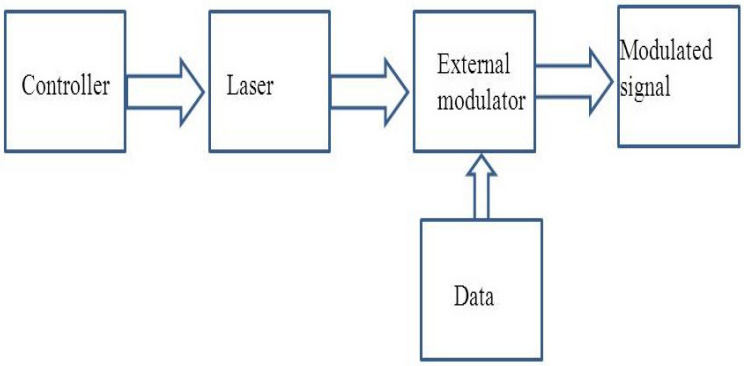


Figure 2.3: Schematic diagram of indirect modulation

This provides electrically controlled on-off transitions that do not affect the light source. The other common method uses electro-absorption (EA) modulators, usually a semiconductor material that can be switched between trans-missive and opaque states to provide the on-off transitions. Materials used in these modulators can be conveniently integrated with the laser diode. As with direct modulation, the driving circuitry uses microwave design and layout to couple high speed data streams to the modulating devices.

2.5.3 Intensity modulation formats

Optical field has three physical attributes which can be used to transmit information, intensity being one of them; phase and polarization are the other

two. In optical communications, intensity modulation (IM) is a form of modulation in which the optical power output of a source is varied in accordance with some characteristic of the modulating signal. The envelope of the modulated optical signal is an analog of the modulating signal in the sense that the instantaneous power of the envelope is an analog of the characteristic of interest in the modulating signal. Recovery of the modulating signal is usually by direct detection, not heterodyne.

2.5.4 Amplitude shift keying

Amplitude shift keying (ASK) is a very popular modulation used in control applications. This is due to its simplicity and low implementation costs. ASK modulation has the advantage of allowing the transmitter to idle during the transmission of a bit zero.This reduces the power consumption. This disadvantage of ASK modulation arises in the presence of an undesired signal. In amplitude shift keying (ASK), as the name specifies the amplitude of the carrier signal is varied between two levels if the ASK scheme is Binary ASK. Sometimes it is more than two levels if the ASK scheme is M-ary. All this is done according to the data bit to be transmitted over the noisy channel. The information is assumed to be uni-polar binary data. In binary ASK bit 1 is transmitted with the carrier of specified amplitude. The bit zero is transmitted with the no carrier during the bit interval. During all the bit intervals amplitude will be changed but frequency will be kept constant. In M-array ask the amplitude levels of the carrier will change between M numbers of values. The main advantage of the ASK is power saving and simplicity in implementation. The ASK wave form can be represented mathematically as $s(t) = m(t)sin(2\pi f_c t)$. where s(t) is the ASK output signal, m(t) is the unipolar binary message signal to be transmitted and f_c is the carrier frequency. Amplitude shift keying (ASK) is a simple and elementary form of digital modulation in which the amplitude of a carrier sinusoid is modified in a discrete manner depending on the value of a modulating symbol. This is a narrow

band modulation scheme and we assume that a large number of carrier cycles are sent within a symbol interval. Obvious that the information is embedded only in the peak amplitude of the modulated signal. This is described as a one type of digital amplitude modulation technique. BASK has only one basis function so this can be described as a one dimensional modulation scheme. This technique is used for telegraph services. On-Off keying is spectraly not efficient scheme because as the amplitude of the carrier changes abruptly when the data bit changes. For this reason this technique is used for transmission of data at low or moderate data rates.

2.5.5 On-Off Keying

On-off keying involves the source transmitting a large amplitude carrier when it wants to send a '1', and it sends a small amplitude carrier when it wants to send a '0' in its simplest form. A further simplification of the ASK method is on-off key (OOK) modulation, in which the source sends NO carrier when it wants to send a '0'. ASK and OOK communication protocols are commonly used in short-range wireless applications.

Non-return-to-zero On-Off Keying (NRZ-OOK)

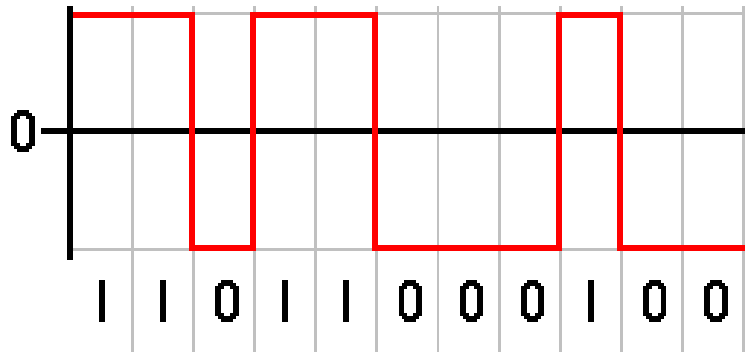


Figure 2.4: The binary signal is encoded using rectangular pulse amplitude modulation with polar non-return to zero code

Non-return-to-zero on-off-keying (NRZ-OOK) has been the dominant modulation format for fiber-optical communication systems. NRZ requires a low electrical bandwidth for the transmitters and receivers, compared to return-to-zero, also it is not sensitive to laser phase noise.

Return-to-zero On-Off keying (RZ-OOK)

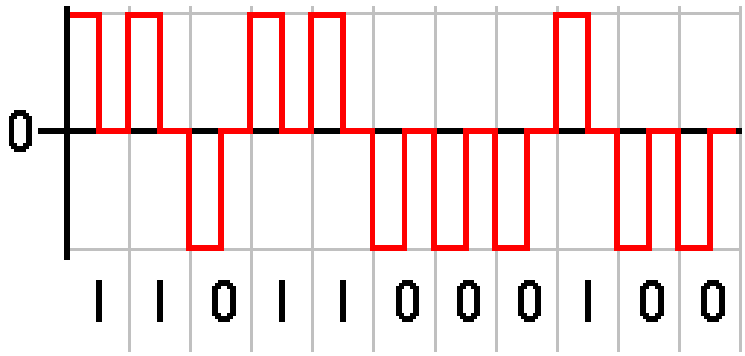


Figure 2.5: The binary signal is encoded using rectangular pulse amplitude modulation with polar return-to-zero code

RZ means return-to-zero, so the width of optical signal is smaller than its bit period. Usually a clock signal with the same data-rate as electrical signal is used to carve RZ shape of optical signals. Figure 2.5 presents the block diagram of a typical RZ transmitter, initially NRZ optical signal is generated by an external intensity modulator; then, it is modulated by a synchronized pulse train with the same data-rate as the electrical signal by cascading another intensity modulator. We can also generate RZ waveforms first and then modulate onto an optical carrier. RZ optical signal has been found to be more tolerant to non-linearity than NRZ optical signal. If the average optical power launched into the fiber is kept constant, an optical RZ pulse with a 50% duty cycle will have twice the peak power of an NRZ pulse. This increase in power occurs because optical amplifiers are run in the saturation mode, resulting in a gain that scales with average input power. The photodiode is a square-law

detector, i.e., the photo-current is proportional to optical power. Hence the received electrical power (proportional to the square of the photo-current) is proportional to the square of the optical power. Therefore, the electrical power of an RZ pulse with a 50% duty cycle will be twice that of an NRZ pulse. RZ formats usually require a slightly more complex transmitter structure, but are generally more robust to ISI.

2.5.6 Pules position modulation

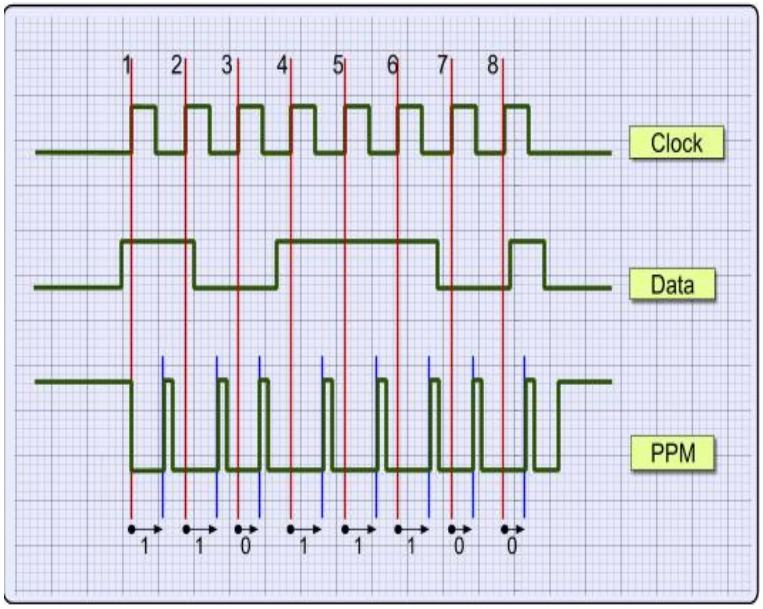


Figure 2.6: Pulse position modulation

Figure 2.6 shows the byte '11011100' is encoded with PPM so that it can be transmitted with infrared light. For the first bit (1), the transmitter will send a pulse 1.8 msec after the rising edge of the clock. For the second bit (1), the transmitter will send a pulse 1.8 msec after the second rising edge of the clock. But for the third bit which is 0, the transmitter will send a pulse after 1.2 msec from the third rising edge of the clock. Same algorithm applies for all other bits[28]. Pulse position modulation (PPM) is common for wired or

wireless communication in fiber optic communications and wireless-optic communications, and PPM is occasionally. In PPM, data are transmitted with short pulses. All pulses have both the same width and amplitude. The parameter that changes is the delay between each pulse. It is obvious that the signal has similar pulses (in terms of amplitude and width), yet the duration between them differs it is widely used in tv remote. In Pulse Position Modulation the amplitude of the pulse is kept constant as in the case of the FM and PWM to avoid noise interference. Unlike the PWM the pulse width is kept constant to achieve constant transmitter power. The modulation is done by varying the position of the pulse from the mean position according to the variations in the amplitude of the modulating signal used for wireless infrared communications.

2.5.7 Phase modulation

Phase modulation is a technique where information encodes in terms of instantaneous phase of a carrier wave. Phase modulation can be used with analog or digital data that makes phase modulation particularly important. It mostly used for transmitting radio signals for a variety of radio communications applications. Phase Modulation (PM) is another form of angle modulation. In both the cases, the total phase angle of the modulated signal varies. As will be seen later, phase modulation, and frequency modulation are closely linked together and it is often used in two way radio communications links, mobile radio communications and even maritime mobile radio communications. In an FM wave, the total phase changes due to the change in the frequency of the carrier corresponding to the changes in the modulating amplitude. In PM, the total phase of the modulated carrier changes due to the changes in the instantaneous phase of the carrier keeping the frequency of the carrier signal constant. These two types of modulation schemes come under the category of angle modulation. However, PM is not as extensively used as FM.

2.5.8 Polarization modulation

Polarization modulation is a technique where information encodes in terms of light polarization. In polarization modulation, the maximum modulation is either right- or left-circularly polarized, while in the other case it is linearly polarized. To effect the improvement in efficiency, the receiver used in a polarization modulation system changes the incident circularly polarized beams to linearly polarized light without the loss introduced by a crossed analyzer. Polarization Modulation Keying is one of the important mechanisms suitable for free space optical communication, but it is often affected by atmospheric effects such as depolarization, attenuation and beam divergence. We shows more detail in chapter 4.

2.5.9 Why Polarization shift keying (PolSK)?

- Amplitude modulation disadvantages: Requires adaptive threshold scheme to perform optimally in the presence of turbulence.
- Phase modulation disadvantages: Highly sensitive to the phase noise, Requires a complex synchronization.
- Frequency modulation disadvantages: Requires more complicated demodulator.
- We further want to extend this setup for free space quantum key distribution (QKD)because BB84 protocol require four state of polarization[29].

2.5.10 Advantage

- Maintains state of polarization (SOP) over a long propagation link in case of free space.
- Doesn't suffer from excess frequency chirp.

- Attractive for the peak power limited systems because its a constant envelope modulation.
- Spectrum is large and license free.
- Installation cost is very low as compared to laying fiber.
- Highly secure transmission possible.
- High data rates, upto 2.5 Gbps at present and 10 Gbps in the near future
- Low bit error rates
- Full duplex operation

2.5.11 Disadvantages

- High Launch Power represents eye hazard.
- Light Interference negatively affects system performance.
- Blockage Leads to design challenges.
- Low Power Source requires high sensitive receivers.
- Alignment Leads to more operation constraints.
- Atmospheric turbulence

2.6 System configuration for PolSK

In the following section we describe our setup to study polarization modulation scheme and discuss each individual component. Figure 2.7 shows block diagram of free space polarization shift keying. Experimental setup consists of two VCSEL's 780nm from Thorlabs and their emission is mixed into a single channel using a polarizing beam (PBS) from Thorlabs. Each VCSEL here in

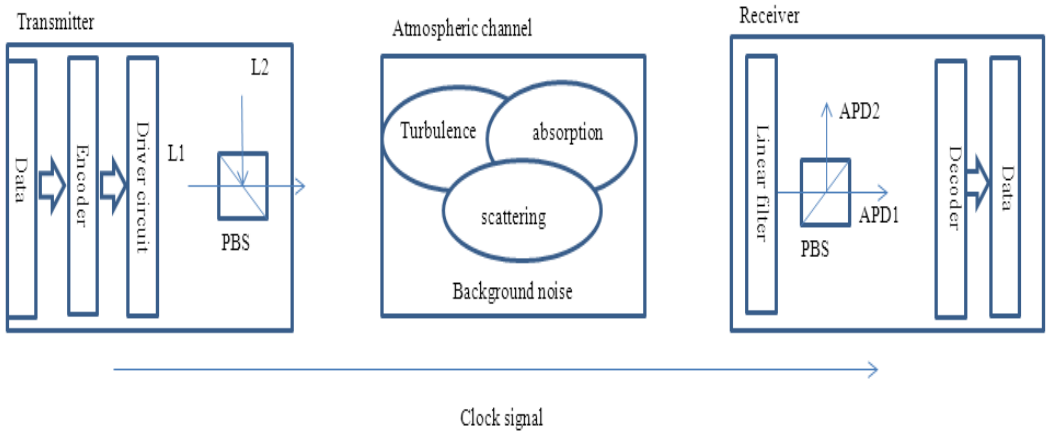


Figure 2.7: Block diagram of experimental setup

denoted as L_1 and L_2, these are represents one bit of information. After the polarizing beam splitter, the beam from L_1 is vertical polarized light and L_2 is horizontal polarized light.

The receiver consists of a PBS and two detectors avalanche photodiode (APD) from sensL. A third laser helps as an external clock pulse to which both transmitter lasers and detectors can be synchronized. A random set of zeros and ones are transmitted using a computer through a DAQ card from National instruments. DAQmx card signal feed in laser controller which is controlling VCSEL lasers. We made program such a way that clock will fire with L_1 and L_2 . Transmitted signal sends in free space which is received by receiver. For better understanding we can divide it in parts.

- Transmitter
- Modulation
- Atmospheric turbulence
- Receiver

According to system configuration and figure 2.7 transmitter consists of several components. Major part is LabVIEW software for controlling physical

device from a computer system and laser diode and modulation. More detail about LabVIEW is explained in chapter 6.

2.6.1 Laser selection

Depending on the systems environment different lasers are used in different types of systems. As far as free space is concerned the highest quality available laser could be effective in every environment. However, as in most things higher precision the higher is the cost. So we try to use the low cost devices that will be adequate in the particular environment.
Factors that need to be considered are:

- Required wavelength and required wavelength stability (how important are wander and chirp etc.)
- Spectral width and linewidth
- Required power output
- Modulation rate required

Based on transmission wavelength in free space from NIST data figure 2.15 maximum transmission is 700 to 800 nm [30]. So we have chosen VCSEL-780nm from Thorlabs .

2.6.2 VCSEL

Vertical Cavity Surface Emitting Lasers (VCSELs) are a relatively recent type of semiconductor lasers. The VCSEL is a technology that has come to great importance in the optical communications field. VCSELs were first invented in the mid 1980s. Very soon, VCSELs gained a reputation as a superior technology for short reach applications such as fiber channel, Ethernet and intra-systems links. Within the first two years of commercial availability (1996),

VCSELs became the technology of choice for short range data communication and local area networks, effectively displacing edge-emitter lasers. This success was mainly due to the VCSELs lower manufacturing costs and higher reliability compared to edge-emitters. Thorlabs has developed a VCSEL with wavelength 780 nm, Power 1.65 mW, Multimode[31]. Below figure 2.8 VCSEL laser diode with four pin extend case,VCSEL anode, VCSEL cathode/PD anode, PD cathode.

Figure 2.8: VCSEL diode

Structure of VCSEL

VCSEL consists of an active layer sandwiched between two highly reflective mirrors (dubbed distributed Bragg reflectors, or DBRs). The active layer is made up of several layers of semiconductors of alternating high and low refractive index, each of about quarter-wavelength-thickness. The light oscillates perpendicular to these layers and escapes through the top or bottom of the device. The mirror and the active region are sequently stached along the y axis during the epitaxial groth see figure2.9.

VCSEL demonstrate excellent dynamic performances such as low threshold currents (a few micro-amps), low noise operation and high-speed digital modulation (10 Gb/s) [32]. Furthermore, although VCSELs have been confined to low-power applications a few milli Watts at most they have the inherent potential of producing very high powers by processing large 2-D arrays. In contrast, edge-emitters cannot be processed in 2-D arrays.

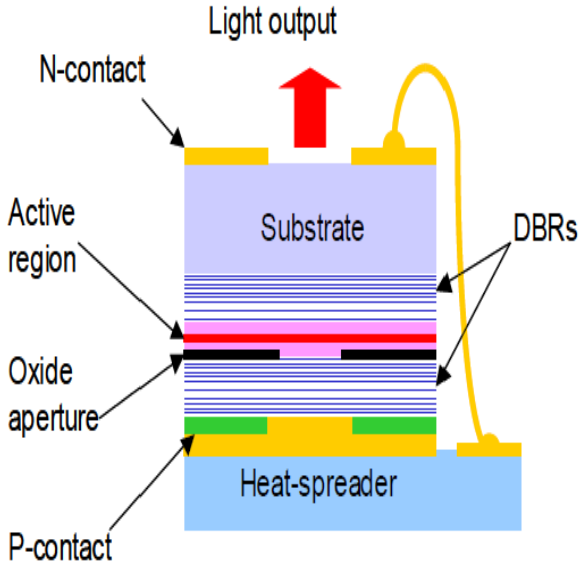


Figure 2.9: VCSEL structure

The optical power out of the VCSEL can be calculated as [33].

$$P_{out} = \eta_i \eta_o \frac{h\upsilon}{q}(I - I_t h) \tag{2.1}$$

where η_i is the injection efficiency, η_o is the optical efficiency, h is Planck constant, υ is the frequency, q is the elementary charge, I is the injected current and $I_t h$ is the current threshold.

V-I characteristic

We observe 5.75mA is the current at which threshold happened as shown in figure 2.10. However, a VCSEL has a ring cavity and hence two modes of operation, with their outputs polarized in two orthogonal polarization. Here we need to measure threshold current for both the component vertical and horizontal polarization.

Figure 2.11 shows the schematic diagram setup for current optical power

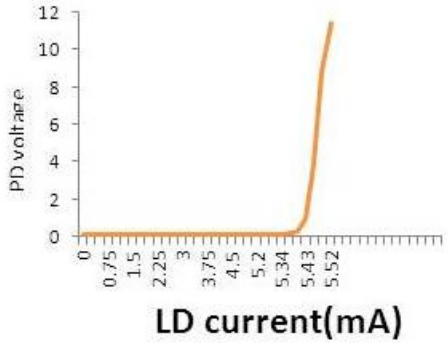


Figure 2.10: The current-optical power relationship

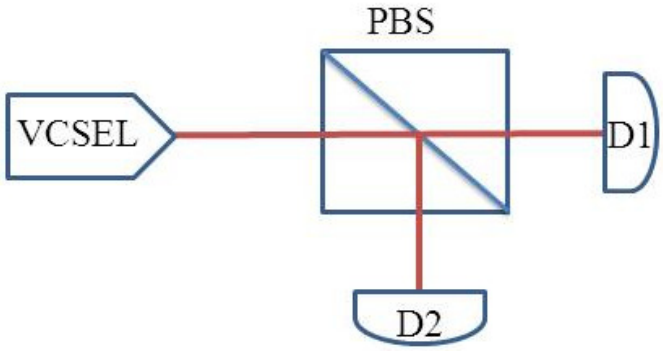


Figure 2.11: Schematic diagram setup for current optical power characteristic

characteristic corresponding output shows in figure 2.12. This shows that VCSEL operation two modes of orthogonal polarization. Different modes dominate at different current since we select our polarization at last stage, we need to operate at polarization insensitive regime,at 5.75 mA.

In figure 2.12 shows polarized component vertical and horizontal with the help of PBS and got lasing current 5.75mA with normal photodiode (SM05PD1A). These tel us operating current of VCSEL.

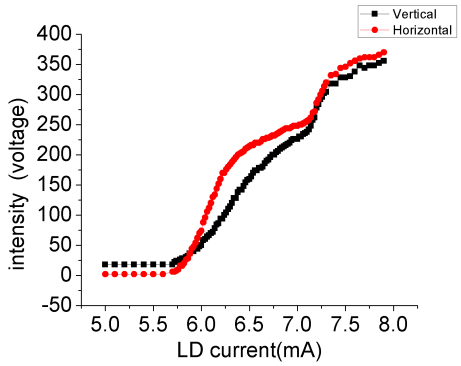


Figure 2.12: The current-optical power relationship of a laser diode using polarization beam splitter

Laser diode polarization:

We have checked the polarization character of our laser beam using stokes parameters. The Stokes parameters are a set of values that describe the polarization state of electromagnetic radiation. The Stokes parameters are defined in terms of the total irradiance of a beam and changes in the irradiance when various polarizers, linear and circular, are inserted in the optical path of the beam figure 2.13[34]. We have measure intensity at six different point by inserting quarter wave plate. Six different measurements of intensity are given below where first place is quarter wave plate (QWP) and second is polarizer place.

- I_1(0,0), Represents intensity with first place QWP position at 0 and second place Polarizer position at 0.
- I_2(0,90)
- I_3(0,45)
- I_4(0,135)
- I_5(90,45)
- I_6(90,135)

In stokes parameter the first parameter expresses the total intensity of the optical field. The remaining three parameters describe the polarization state.

- $S_0 = I_1 + I_2$
- $S_1 = I_1 - I_2$
- $S_2 = I_3 - I_4$
- $S_3 = I_6 - I_5$

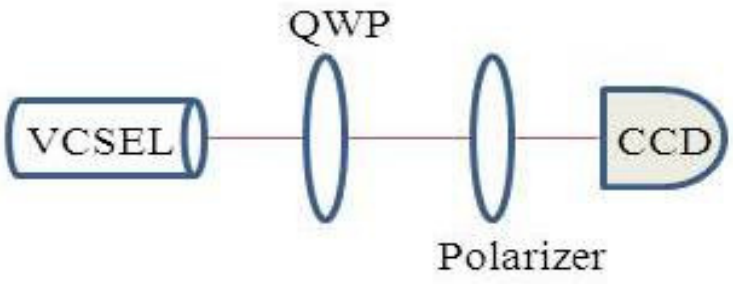


Figure 2.13: Schematic diagram of experimental setup

Condition for stoke parameter

- if $S_1 = \pm 1$ and others are zero linear polarized (vertical or horizontal) light
- if $S_2 = \pm 1$ and others are zero linear polarized (45 or 135) light
- if $S_3 = \pm 1$ and others are zero circular polarized light
- if all are non zero unpolarized light

The images taken by the CCD for different positions of the quarter wave plate, denoted q_i and p_j are shown in figure2.14. a MATLAB programs is used to compute the stokes parameters at each pixel. These result with false coloring to indicate the value is also shown in figure2.14. From these it can be noticed the at current 5.7 mA, the VCSEL gives a partially polarized light.

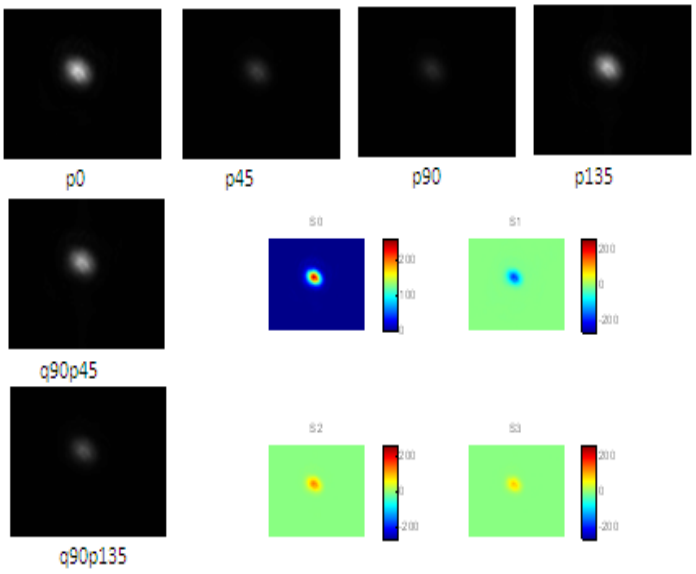


Figure 2.14: Intensity profile based on stokes parameter

Advantages of VCSEL

The many advantages offered by the VCSEL technology can be summarized in the following points:

1. Lower divergence
2. Circular cross-section that can be easily coupled.
3. Low current needed due to small active volume
4. The lasing wavelength in a VCSEL is very stable, since it is fixed by the short (1 to 1.5 μm wavelength thick) Fabry-Perot cavity. Contrary to edge-emitters, VCSELs can only operate in a single longitudinal mode.
5. Since the emission wavelength in VCSELs depends upon the optical thickness of the cavity, the emission wavelength is less sensitive to temperature variations than in edge-emitters. On the other hand, the lasing wavelength in edge emitters is defined by the peak-gain wavelength, and hence a stronger on temperature.

6. VCSEL devices can be operated without refrigeration because they can be operated at temperatures to 80 deg C, the cooling system becomes very small, rugged and portable with this approach.

7. VCSELs emit a circular beam. Through proper cavity design VCSELs can also emit in a single transverse mode (circular Gaussian). This simple beam structure greatly reduces the complexity and cost of coupling/beam-shaping optics (compared to edge-emitters) and increases the coupling efficiency to the fiber or pumped medium. This has been a key selling point for the VCSEL technology in low-power markets.

8. Because VCSELs are not subject to catastrophic optical damage (COD), their reliability is much higher than for edge-emitters. Typical FIT values (failures in one billion device-hours) for VCSELs are < 10.

2.7 Atmospheric turbulence

The atmosphere is a dynamic medium with a randomly varying refractive index to a propagating laser beam. An optical radiation propagating through the atmospheric channel is subject to atmospheric attenuation due to the photons absorption and scattering by the molecular constituents (ozone, fog,smoke etc.) [3, 10, 14, 35]. Since their dimensions are very close to the wavelengths of the optical signals[36]. However, in terms of evaluation of different weather conditions, fog and smoke are considered to be the dominant aerosol particles that could potentially disrupt the communications by attenuating the input optical signal to the receiving side [37]. Therefore, the chemical compositions of these types of aerosols in terms of particle size and visibility range are the important factors to understand their effects on the propagating optical beam [38, 39, 40, 41]. When some of the photons are extinguished, their energies turn into heat [5]. The earth absorbs solar radiation and radiates the heat through the air around the earth surface and become warmer at higher altitudes. Hence, warmer air being lighter rises to mix turbulently with the surrounding cooler

air causing the air temperature to fluctuate randomly. Turbulence is caused by the temperature inhomogeneities presents in the atmosphere . This can be understand as indices of different sizes with changing temperatures floating in the air. The direction of an optical beam could be altered due to interaction with discrete cells of variable temperatures, or eddies, acting like prisms with different refractive indices, thus resulting in fluctuation of the received optical signal amplitude variations (i.e.,scintillation) and random phase changes [42]. This leads to reduction in signal intensity of an information-bearing optical beam, which ultimately results in performance degradation of FSO links [43]. The atmospheric turbulence depends on the wind speed, the atmospheric altitude/pressure, and the variation of refractive index.

The optical radiation also experiences scattering, which changes the initial propagating direction, shape, and electromagnetic properties of the laser. Furthermore, the beam also spreads out while propagating over the channel, thus enlarging the received power footprint which becomes larger than the detector aperture area [44]. Atmospheric scattering causes the angular fluctuations. The optical radiation is scattered due to the molecular size particles and this process is called Rayleigh scattering. When particle (fog and smoke) size is large compared with the transmission wavelength, the process is called Mie scattering. Mie scattering is much less wavelength dependent while Rayleigh scattering is predominant at the shorter wavelengths [45, 46, 47].

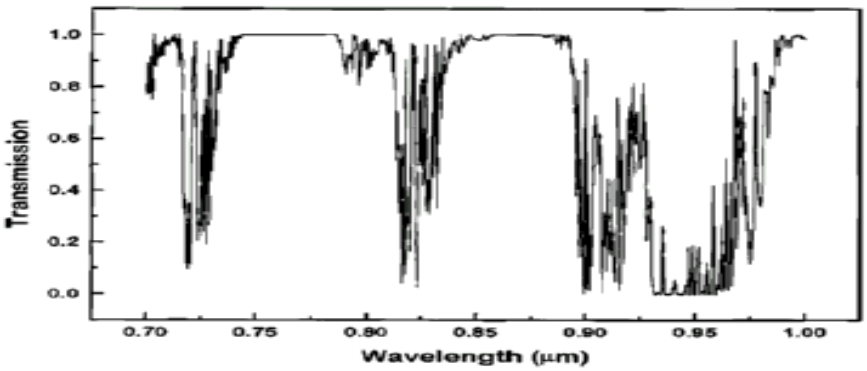


Figure 2.15: Transmission loss in free space

The atmospheric molecular concentration depends on the pressure and temperature that vary with weather, altitude, and geographical locations. Absorption varies as the function of wavelength. This is only IR region, see figure 2.15 the absorption windows along the spectral regions corresponding to the visible and the near-infrared radiations are approximately 700 to 980 nm, 1.1 to 1.6 m, 1.3 to 1.5 m, and 1.8 to 2 m. The wavelengths used in outdoor wireless systems are selected to coincide with the absorption windows, such as 780 to 800 nm, 1.2 to 1.3 m, and 1.5 to 1.7 m [48, 49]. In clear weather conditions, apart from attenuation, the laser beam traversing the atmospheric channel also experiences the atmospheric turbulence [3, 8, 22, 50, 51].
The influences of atmospheric turbulence on the laser communications include:

- Beam steering - Angular deviation of the beam from its initial LOS target leading to the beam being out of the receiver aperture range.
- Image dancing - The focus of the received beam moves randomly in the image plane caused by the variations of the arrival-angle of the laser.
- Beam spreading - The beam divergence is increased due to scattering, which causes a reduction in the received power density.
- Beam scintillation - The spatial power density fluctuates at the receiver plane which is the result of small scale destructive interference within the optical beam cross section.
- Spatial coherence degradation - The phase coherence across the beam phase fronts suffers losses due to the turbulence

2.7.1 Fog composition

Fog is the composition of very fine water particles suspended in the air forming a cloud near the ground. The formation of the water particles takes place mainly due to the evaporation of liquid water or by the sublimation of ice, where the state of ice changes into vapors. The thickness of fog is largely

determined by the altitude or the distance of the inversion boundary [52]. In principle, fog particles reduce the visibility near the ground and the meteorological definition of fog is when the visibility drops to near 1 km. Depending on how fog is formed there are a number of different fog types as reported in [53] as discussed below. Convection or Radiation fog is generated due to

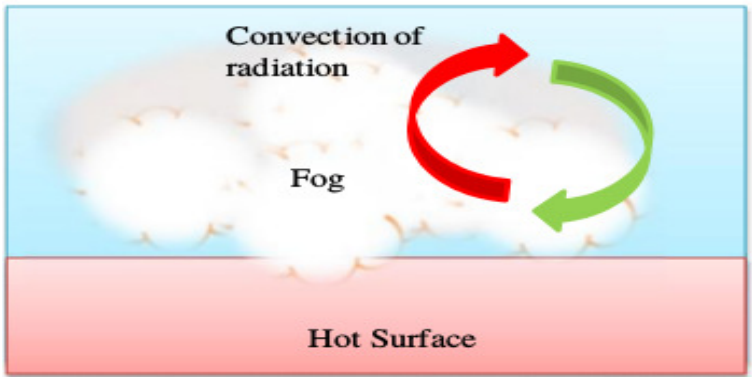


Figure 2.16: The mechanism of convection fog formation

the ground cooling by radiation. This type of fog appears when the air is sufficiently cool and becomes saturated due to convection of hot radiations by cooling down the surface as illustrated in Figure 2.16. Principally, convection appears during the night and at the end of the day with the particle diameters for this type of fog presents a weak variation around 4 m and the liquid water content varies between 0.01 and 0.1 g/m^3. A common visibility range for this type of fog is 0.5 km. Mostly, the radiation fog falls during early winter and is considered to be dense and localized.

Advection fog occurs by the movement of wet and warm air masses above the colder maritime or terrestrial surfaces as described in Figure 2.17. This type of fog is characterized by the liquid water content, higher than 0.20 g/m^3 and with a particle diameter close to 20μm. A common visibility range is 0.2 km for the advection fog The precipitation fog falls when fine rain falls into dry air below the cloud and the droplets shrink into vapours. The water vapours cool down and at the dew point, it condenses to form fog. The valley fog forms in mountain valleys as a result of temperature inversion. It can last for

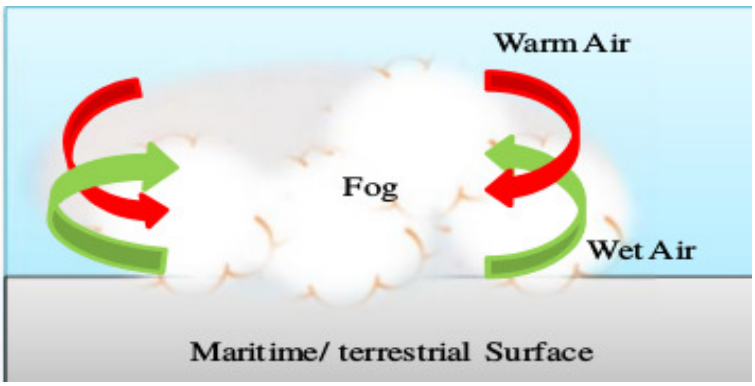


Figure 2.17: The mechanism of advection fog formation

several days in still conditions. Valley fog is also known as tule fog [54]. Steam fog is localized and is created by cold air passing over much warmer water or moist land [55]. Power plants that emit large quantities of steam may also be included in this category for real fog. Any visibility setting that ranges from 0 km to 1 km is reasonable for water based steam fog [55].

2.7.2 Smoke composition

Smoke is generally formed in Real outdoor atmosphere (ROA) from the combustion of different substances such as carbon, glycerol and house hold emission [54]. Smoke is considered to be a visible gaseous substance in which small dry solid particles stays and disperse in the atmosphere for long time. It is commonly an unwanted by- product of fires and fireplaces, however, can also be used for pest control and communication as smoke signals [56]. The most common method for smoke suspension measurements today employs a light source and a photoelectric, arranged such that the electrical output of the light source may be used as a measure of the attenuation of light by smoke. Scattering measurements are generally limited to particles whose size is of the order of the wavelength of visible light. However, since the aim is measurement of smoke as it relates to the visibility, the light attenuation method appears to be the most direct. The scattering of the optical beam depends on the refractive index of

the material used for the smoke particles.

2.7.3 Characterization of fog and smoke attenuation theoretical approach

Assuming the shape of the aerosol particles is spherical presenting in the Real Outdoor Atmosphere (ROA), mainly those constituting the fog. The exact Mie theory can be applied to measure the scattering and absorption cross sections of the particles. Mie theory determines the scattered electromagnetic field by homogeneous spherical particles by calculating the Mie scattering and absorption cross sections of the particles defined by [57]

$$C_s = \frac{P_s}{I_0} \tag{2.2}$$

$$C_a = \frac{P_a}{I_0} \tag{2.3}$$

where P_s (W) is the electromagnetic power scattered across the surface of an imaginary sphere centered on the particle, P_a(W) is the electromagnetic power absorbed across the surface of an imaginary sphere cantered on the particle, and I_o(W/ m^2) is the intensity of the incident radiation. The FSO wavelengths are mostly selected in the atmospheric transmission windows, where the molecular absorption due to gases is considered to be negligible, i.e. ($C_a \approx 0$) using (2.2). In principle, the selection of the wavelength in FSO communications can be selected using the wavelength windows of 0.69, 0.85 and 1.55 μm in order to minimize the absorption coefficient. The normalized cross section or absorption efficiency Qa can be defined as [58]

$$Q_a = \frac{C_a}{\pi r^2} \tag{2.4}$$

However, considering fog and smoke, the major contribution in the attenuation is due to the scattering of the optical signal due to the Mie scattering. In order

to calculate the attenuation due to Mie scattering, the value of the normalized cross section or scattering efficiency Qs must be known. It is defined by [57, 58]

$$Q_s = \frac{C_s}{\pi r^2} \tag{2.5}$$

The Q_s is the function of the size parameter (r/λ) unitless quantity, the maximum value of the normalized scattering cross section reaches to 3.8 at r/$\lambda \approx$ 1 i.e. maximum scattering of the optical signal [59]. However, the particle radius r of the fog varies in the spatial domain in the atmosphere. Due to the lack of the fixed particle size along the length of the FSO link, we may have different values of Q leading to the total attenuation due to the fog. The total attenuation β_λ of the optical signal due to the scattering and absorption coefficients γ_λ and α_λ, respectively of fog is given by [60]

$$\beta_\lambda = \gamma_\lambda + \alpha_\lambda = \int_0^\infty \pi r^2 Q_s(\frac{2\pi r}{\lambda}, n) n(r) \mathrm{d}r + \int_0^\infty \pi r^2 Q_a(\frac{2\pi r}{\lambda}, n') n(r) \mathrm{d}r \tag{2.6}$$

Where n represents the real part of the refractive index, which depends on the material composition of the fog, in the case of water based fog n is wavelength dependent from visible NIR spectrum [61]. However, $n^{`}$ represents the imaginary part of the refractive index, which contributes toα_λ due to the fog particles. In general values of n' for the water based particles are very small for the visible NIR wavelengths compared to the FIR as can be ignored. Here $\frac{2\pi r}{\lambda}$ is the size parameter that depends on the incident λ and r. N(r) is the particle size distribution function of the aerosols and is an important parameter to determine the physical and optical properties of the fog [59, 61].

2.7.4 Atmospheric transmittance

To quantify laser beam attenuation experienced by an optical communications link, one can introduce the concept of optical depth τ. The power reaching

the receiver P(r) is related to the transmitted power P(t) [62] as

$$P(r) = P(t)e^{-\tau} \tag{2.7}$$

The fraction of the power transmitted in the optical link, T, is called transmittance and is given by

$$T = \frac{P(r)}{P(t)} = e^{-\tau} \tag{2.8}$$

The atmospheric transmittance and the optical depth are related to the atmospheric attenuation coefficient gamma and the transmission path length r by

$$T = e^{-\int_0^r \gamma(\rho)\,\mathrm{d}\rho} \tag{2.9}$$

where

$$\tau = \int_0^r \gamma(\rho)\,\mathrm{d}\rho \tag{2.10}$$

where the atmospheric attenuation coefficient is laser-wavelength specific and depends on the path-integrated distribution of atmospheric constituents along the line-of-sight. From the above equation, one can define the loss L in decibels that the beam experiences as

$$L = -10\log(T) \tag{2.11}$$

Generally speaking, the atmospheric attenuation coefficient can be expressed as the combination of absorption and scattering of the light beam due to gas molecules and aerosols present in the atmosphere:

$$\gamma = \alpha(a) + \beta(m) + \alpha(a) + \beta(a) \tag{2.12}$$

where $\alpha(m)$ and $\alpha(a)$ are respectively the absorption coefficient for the molecular gas and aerosol, and $\beta(m)$ and $\beta(a)$ are the scattering coefficient for the molecular gas and aerosol. One should notice that although both absorption and scattering contribute to the attenuation coefficient, their attenuation

mechanism is quite different. Generally, scattering can be classified according to the size of the scattering particle and the wavelength: if the scattering particle is smaller than the wavelength the process is termed Rayleigh scattering [63]; if the size of the scatterer is comparable to the wavelength, it is termed Mie scattering [64]. Commonly, one may observe that molecular scattering is due to Rayleigh scattering while aerosol scattering is better described by Mie theory. When the size of the scatterers is much larger than the wavelength in consideration, diffraction theory can describe the scattering of light in a more proper fashion.

2.8 Receiver

From figure 2.7 receiver detects light signal by using detector and extracts the information. Coming paragraph I am explaining more about detector.

2.8.1 Photodiode

A photodiode is a semiconductor device that converts light into current or voltage depending upon the mode of operation. The current is generated when photons are absorbed in the photodiode. A small amount of current is also produced when no light is present. Photodiodes may contain optical filters, built-in lenses, and may have large or small surface areas. Photodiodes usually have a slower response time as its surface area increases.

Principle of operation

A photodiode is a PN junction or PIN structure. When a photon of sufficient energy strikes the diode, it excites an electron, thereby creating a free electron and a (positively charged electron) hole. If the absorption occurs in the junction's depletion region, or one diffusion length away from it, these carriers are swept from the junction by the built-in field of the depletion region.

Thus holes move toward the anode, and electrons toward the cathode, and a photo-current is produced.

Photovoltaic mode

When used in zero bias or photo-voltaic mode, the flow of photo-current out of the device is restricted and a voltage builds up. The diode becomes forward biased and "dark current" begins to flow across the junction in the direction opposite to the photo-current. This mode is responsible for the photo-voltaic effect, which is the basis for solar cells in fact, a traditional solar cell is just a large area photo-diode.

Photo-conductive mode

In this mode the diode is often reverse biased (with the cathode driven positive with respect to the anode). This reduces the response time because the additional reverse bias increases the width of the depletion layer, which decreases the junction's capacitance. The reverse bias also increases the dark current without much change in the photo-current. For a given spectral distribution, the photo-current is linearly proportional to the illuminance (and to the irradiance)[65]. Although this mode is faster, the photo conductive mode tends to exhibit more electronic noise. The leakage current of a good PIN diode is so low ($< 1nA$) that the Johnson Nyquist noise of the load resistance in a typical circuit often dominates.

2.8.2 Avalanche photodiode

In our setup, we mainly use APD's in counter mode. Avalanche Photo-diodes (APDs) are high sensitivity, high speed semiconductor light sensors. Due to physical properties most detectors are only efficient in limited wavelength window figure 2.18 shows quantum efficiency obtain for different detector [66]. Compared to regular PIN construction photo-diodes, APDs, have an internal

region where electron multiplication occurs, by application of an external reverse voltage, and the resultant gain in the output signal means that low light levels can be measured at high speed. Incident photons create electron hole pairs in the depletion layer of a silicon photo-diode structure. APD gain is typ-

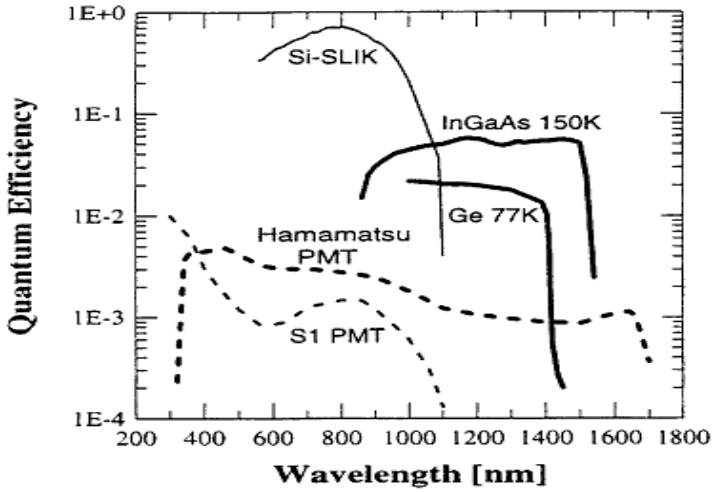


Figure 2.18: Quantum efficiency of various dectectors [66]

ically in the range from x10 to x300 for most commercial devices, but there are APDs available from specialist manufacturers with gains of thousands. This then can give a significant advantage over regular PIN photodiodes for applications which are short of photons and where it is not possible to integrate these low signals. As with regular photodiodes the maximum wavelength than can be detected is determined by the semiconductor band gap energy using the formula, which is 1.12 eV for silicon at room temperature, giving a cut-off at 1100 nm. At longer wavelengths then an alternative semiconductor material with smaller band gap is required, such as Germanium, or much more commonly these days due to its higher performance, InGaAs is chosen. Avalanche Photodiodes fabricated from these materials are then available in the market for operation in the 900 nm to 1700 nm wavelength range. A wide range of silicon APDs are commercially available, in sizes from <100 microns diameter

to several cm diameter. The peak wavelength for silicon APDs tends to be from 600 nm to 800 nm, some what shorter than the 900 nm to 1000 nm peak wavelength for a regular photodiode.

All semiconductor devices have such an associated dark current caused by thermal (rather than optical) generation of electron holes. In practice then the shot noise associated with this dark current ultimately will limit the minimum amount of light that any device can detect. Thermoelectric cooling can then reduce the dark current and thus improve the range of incident light that can be measured. The shot noise of an APD is higher than that for a comparable performance photodiode, so even though the APD gives an amplified output the overall signal to noise performance (SNR) is not necessarily improved. In order for a regular photodiode to detect lower light levels it is usual to increase the gain in the operating circuit by increasing the feedback resistor value. But this has the unwanted consequence of reducing the speed of response and increasing the thermal noise associated with the operating circuit. In contrast, operation with an APD allows for the gain to be increased to improve the SNR whilst maintaining the speed of response, until the shot noise reaches a level equivalent to the thermal noise. As the APD gain increases the output signal increases linearly, but the noise increases as shown in the graph 2.19. This means for any APD there is an optimum operating gain, usually well below the actual maximum gain for that APD, where the maximum signal to noise performance can be obtained. Usually pre-set by the manufacturers optimum performance is apparent that the shot noise of an APD is higher than that for a comparable performance photodiode, so even though the APD gives an amplified output the overall signal to noise performance (SNR) is not necessarily improved[67]. To improve the SNR whilst maintaining the speed of response, gain to be increased until the shot noise reaches a level equivalent to the thermal noise.

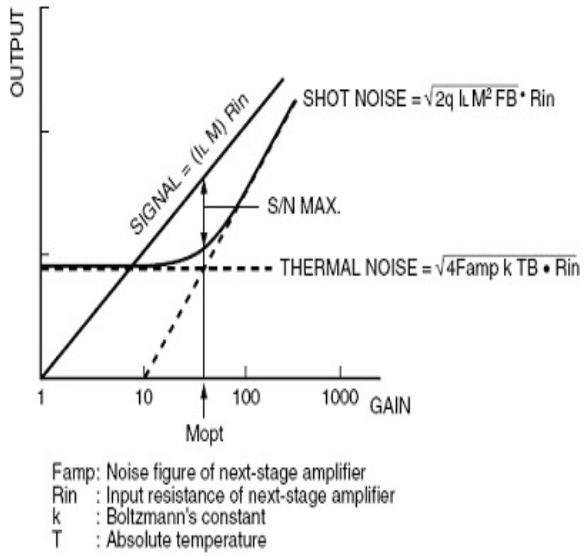


Figure 2.19: Gain vs output [67]

SensL PCDmini

We used PCDmini from SensL for our experties. This is an integrated module consisting of APD, temprature controller and USB coupller. The PCDMini sensing performance exceeds typical photomultiplier tubes (PMT) values for key photon counting parameters such as photon detection probability, dark count, timing jitter and after pulsing. Figure 2.20 is a Integrated module for APD from sensL company.

Features applications

- Miniaturized photon counting solution for OEM and Researchers.
- Not damaged by excess / ambient light.
- Controlled thermoelectric cooling for applications that require cooling for extremely low dark count.
- USB 2.0 (full-speed) interface board.

Figure 2.20: APD module

- Power supply board and included wall mount supply provide all power required by the PCDMini.

2.8.3 Geiger-mode avalanche photo-diodes

As the bias voltage applied to APD is increased approaching the breakdown voltage of the device the gain begin to increases rapidly. As breakdown approaches the gain becomes so great that only a few primary carriers required to generate a self-sustaining avalanche current. Once the device is biased above the breakdown the electric field is close to critical breakdown field for semiconductor and a single charge carriers entering the depletion region of the device is sufficient to cause a self sustaining avalanche current to be generated. The magnitude of the avalanche current is limited only by the reverse on resistance of the device and any external resistance connected to the device. The Geiger mode (above breakdown) the detector becomes very sensitive to single photon of light[68].

2.8.4 Noise in photo-diodes

Noise is generally an unwanted and undesirable component making up part of the overall signal measured by the detector. Usually the noise is a random fluctuation the is not related to the signal that what we wish to measure. There

are different types of detector that we could explore, but here we limit ourselves to a discussion of noise in photo conductive, p-n junction and avalanche photodiodes. The main source of noise that we will discuss are.

Johnson noise

Johnson noise some times called Nyquist Noise, is the electronic noise generated by the thermal agitation of the charge carriers (usually the electrons) inside an electrical conductor at equilibrium, which happens regardless of any applied voltage. The generic, statistical physical derivation of this noise is called the fluctuation-dissipation theorem, where generalized impedance or generalized susceptibility is used to characterize the medium[69]. The mean square Johnson noise current is given by

$$i_j^2 = \frac{4kTB}{R}$$

where k is Boltzmann's constant , T is the absolute temperature, B is the signal bandwidth, and R is the resistance.

Shot noise

Shot noise in photodiode occurs due to statistical fluctuation in the photocurrent caused by the random arrival times of photon absorbed to create the e-h pairs [68].

Flicker noise

This arises from surface and interface defects and traps in the bulk of semiconductor and is only important at very low frequency typically less than 1kHz.

Escess noise in avalanche photodiode

Avalanche Photodiode, biased in avalanche mode, suffer from shot noise connected with the unmultiplied signal, dark and background current. The main

noise source in APD is itself the avalanche process that provides the gain in the device. The avalanche process is a probabilistic one, in that there is random fluctuation in the distance between successive ionizing collision. The nature of these variations such that there are fluctuation in the number of secondary carriers generated per primary carrier injected into the gain region of the device. this fluctuation leads to an excess noise in the total signal current.

2.9 Theoretical aspect of experimental system

In our experiment we study some of the polarization effects and how obstacle can change the polarization of a light beam. We can represent the two orthogonal components of a plane electromagnetic wave traveling in the z direction in the form

$$E_x(z,t) = \hat{i}E_{0x}\ cos(kz - \omega t) \tag{2.13}$$

$$E_y(z,t) = \hat{j}E_{0y}\ cos(kz - \omega t + \phi) \tag{2.14}$$

where ϕ is the relative phase of the two components $\hat{i}$ and $\hat{j}$ are unit vectors in orthogonal direction. The total field is the vector sum of the two components, $E = E_{0x} + E_{0y}$. The state of polarization depends on ϕ and the relative magnitudes of E_{0x} and E_{0y}.

2.9.1 Linear polarized light

Linear polarization occurs when $\phi = 0$ or is an integral multiple of $\pm\pi$ and amplitude $E_{0x} = E_{0y}$. The tip of the field vector follows a sine curve in a plane containing the direction of propagation, and therefore traces a straight line in a fixed plane perpendicular to the direction of propagation. Figure 2.21 shows linearly polarized light.

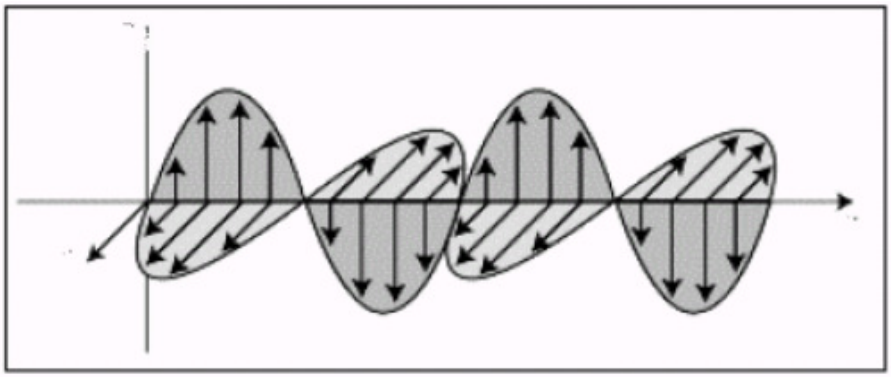


Figure 2.21: Linearly polarized light at 45^0

2.9.2 Circular polarized light

Left-hand circular polarization (LHC) occurs when $\phi = \pi/2 + 2m$ (where m = 0, ±1, etc) and $E_{0x} = E_{0y}$. Now the tip of the field vector follows a circular helix around the direction of propagation, and traces out a circle in the perpendicular plane. Looking into the beam the vector rotates counter-clockwise around its circle. Similarly, right hand circular polarization (RHC) occurs when $\phi = -\pi/2 + 2m$ (where m = 0, ±1, etc) and $E_{0x} = E_{0y}$which looks just like LHC except that the sense of rotation is reversed to be clockwise looking into the beam. Figure 2.22 is showing circularly polarized light.

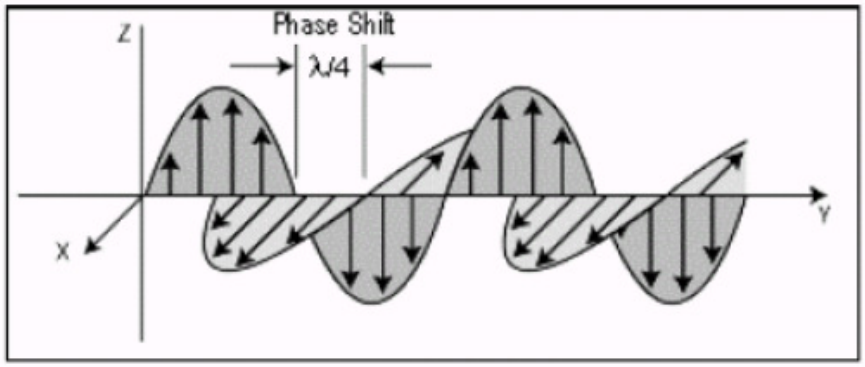


Figure 2.22: Circularly polarized light

2.9.3 Elliptical polarized light

For most values of $\phi = \pm\pi$ and the two amplitudes $E_{0x} \neq E_{0y}$ the light beam is said to be elliptically polarized. This means that the end of the electric field vector traces out an ellipse as the wave moves through a fixed plane normal to the propagation direction. Figure 2.23shows elliptically polarized light.

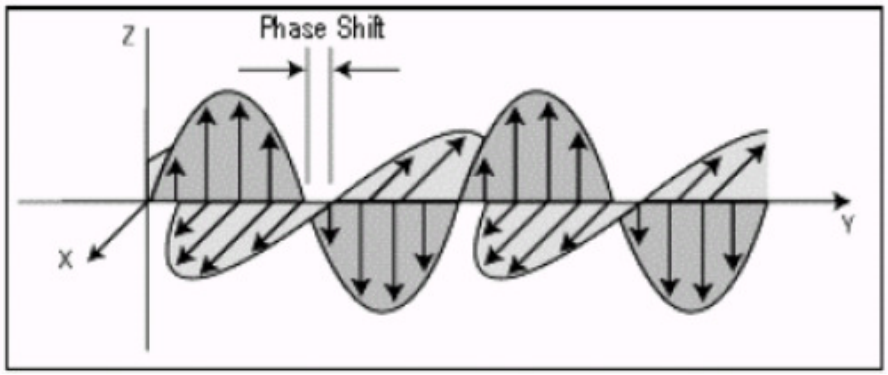


Figure 2.23: Elliptically polarized light

2.10 Conclusions

The main focus of this chapter is to explain basic concept of free space optical communication. The experimental setup for PolSK is introduced, and the functions of individual parts are highlighted. The atmospheric channel and the noise sources that limit the data transmission are described. We explain basic concept of VCSEL laser and characterize it. Descriptions of the operating principles of modulation were given. We explain light polarization in free space and also given basics concept of Avalanche photo diode.

Bibliography

[1] T. Plank, M. Czaputa, E. Leitgeb, S. S. Muhammad, N. Djaja, B. Hillbrand, P. Mandl, and M. Schonhuber, "Wavelength selection on FSO

links", Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP), pp. 2508-2512, 2011.

[2] S. A. J. Fl rez, "Circular polarization and availability in free space optics (FSO) communication systems", IEEE Latin-American Conference on Communications (LATINCOM) 2010, pp. 1-6, 2010.

[3] M. Niu, J. Cheng, and J. F. Holzman, "Diversity reception for coherent free-space optical communications over K-distributed atmospheric turbulence channels",IEEE Wireless Communications and Networking Conference (WCNC) 2010, pp. 1-6, 2010.

[4] Fatin Hamimi Mustafa, Abu Sahmah M Supaat, Nachimani Charde, "Effect of Rain Attenuations on Free Space Optic Transmission in Kuala Lumpur", Proceeding of the International Conference on Advanced Science, Engineering and Information Technology, 2011.

[5] W. O. Popoola, "Subcarrier intensity modulated free-space optical communication systems," in School of Computing, Engineering and Information Sciences. vol. Doctor of Philosophy Newcastle: University of Northumbria, September 2009, p. 264.

[6] E. Ciaramella, Y. Arimoto, G. Contestabile, M. Presi, A. D'Errico, V. Guarino, and M. Matsumoto, "1.28 terabit/s (32x40 Gbit/s) WDM transmission system for free space optical communications," IEEE Journal on Selected Areas in Communications vol. 27 pp. 1639 - 1645, 2009.

[7] T. Yamashita, M. Morita, M. Shimizu, D. Eto, K. Shiratama, and S. Murata, "The new tracking control system for free-space optical communications," International Conference on Space Optical Systems and Applications (ICSOS), pp. 122-131, 2011

[8] X. Wu, P. Liu, and M. Matsumoto, "A study on atmospheric turbulence effects in full-optical free-space communication systems," 6th Inter-

national Conference on Wireless Communications Networking and Mobile Computing 2010 (WiCOM), pp. 1-5, 2010.

[9] A. C. Boucouvalas, "Editorial," EURASIP Journal on Wireless Communications and Networking 2005, vol. 2005, pp. 1-2, 2005.

[10] E. Dadrasnia, S. Ebrahimzadeh, and F. R. M. Adikan, "Inuence of short range free space optical atmospheric attenuation in modulated radio signal," The 2nd International Conference

[11] A. Bekkali, C. B. Naila, K. Kazaura, K. Wakamori, and M. Matsumoto,"Transmission analysis of OFDM-based wireless services over turbulent radio-on-FSO links modeled by gamma-gamma distribution," IEEE Photonics Journal, vol. 2, pp. 510-520, 2010

[12] N. H. M. Noor, A. W. Naji, and W. Al-Khateeb, "Theoretical analysis of multiple transmitters/receivers on the performance of free space optics (FSO) link," IEEE International Conference on Space Science and Communication 2011, pp. 291- 295, July 2011.

[13] P. P. Smyth, P. L. Eardley, K. T. Dalton, D. R. Wisely, P. McKee, and D. Wood, "Optical wireless: a prognosis," Proceeding of SPIE, vol. 2601, pp. 212-225, 1995.

[14] S. A. Zabidi, W. A. Khateeb, M. R. Islam, and A. W. Naji, "Investigating of rain attenuation impact on free space optics propagation in tropical region," 4th International Conference On Mechatronics 2011, pp. 1-6, 2011.

[15] M. Gregory and S. Badri-Hoeher, "Characterization of maritime RF/FSO channel," International Conference on Space Optical Systems and Applications (ICSOS) 2011, pp. 21-27, 2011

[16] Bloom, S. (2002). The Physics of Free-Space Optics. AirFiber Inc.1-22.

[17] L. C. Andrews, R. L. Phillips, and C. Y. Hopen," Laser Beam Scintillation with Applications", SPIE Press, Bellingham; Washington, DC, 2001

[18] A. K. Majumdar, Free Space Laser Communication Performance in the Atmospheric Channel, J. Opt.Fiber. Commun. Rep. 2 (4), 345396 (2005).

[19] M. A. Vorontsov Bit Error Rate in Free Space Optical Communication Systems with a Partially Coherent Transmitting Beam ISSN 1024-8560, Atmospheric and Oceanic Optics, Vol. 26, No. 3, pp. 185189, 2013

[20] Xuan tang "POLARISATION SHIFT KEYING MODULATED FREE-SPACE OPTICAL COMMUNICATION SYSTEMS" University of Northumbria at Newcastle,2012.

[21] Z. X. Wang, W. D. Zhong, S. N. Fu, and C. Lin, "Performance comparison of different modulation formats over free-space optical (FSO) turbulence links with space diversity reception technique," IEEE Photonics Journal, vol. 1, pp. 277-285, December 2009

[22] X. Zhu and J. M. Kahn, "Free-space optical communication through atmospheric turbulence channels," IEEE Transactions on Communications, vol. 50, pp. 1293-1300, August 2002

[23] W. Gappmair and M. Flohberger, "Error performance of coded FSO links in turbulent atmosphere modeled by Gamma-Gamma distribution", IEEE Trans. Wireless Commun., vol. 8, no. 5, pp. 22092213, May 2009

[24] N. Letzepis, I. Holland, and W. Cowley, "The Gaussian free space optical MIMO channel with Q-ary pulse positionmodulation", IEEE Trans. Wireless Commun., vol. 7, no. 5, pp. 17441753, May 2008

[25] I. B. Djordjevic, B. Vasic, and M. A. Neifeld, "Multilevel coding in free-space optical MIMO transmission with Q-ary PPM over the atmospheric turbulence channel", IEEE Photon. Technol. Lett., vol. 18, no. 14, pp. 14911493,Jul. 15, 2008

[26] N. Letzepis and A. G. Fabregas, "Outage Probability of the Gaussian MIMO Free-Space Optical Channel With PPM",Online Available: http://arxiv.org/abs/0804.0050

[27] K. Kiasaleh, "Performance of coherent DPSK free-space optical communication systems in K-distributed turbulence", IEEE Trans. Commun., vol. 54, no. 4, pp. 604607, Apr. 2006

[28] $http://www.pcbheaven.com/wikipages/Pulse_{P}osition_{M}odulation/$

[29] Bennet C. and Brassard G., Proceedings of IEEE conference and computers, systems and signal processing, Bangalore,India, 1984.

[30] Nicolas Gisin, Gre goire Ribordy,"Quantum cryptography "REVIEWS OF MODERN PHYSICS, VOLUME 74, JANUARY 2002.

[31] http://www.thorlabs.com/thorproduct.cfm?partnumber=VCSEL-780

[32] Kimble H.J. and Mandel L, "Spatial coherence of laser output far below threshold",JOSA 63, 1550,1973

[33] L. A. C. S. W. Corzine," Diode Laser and Photonic Integrated Circuits", Wiley, 1995.

[34] Optics by Hecht and Polarized Light by Shurcliff.

[35] M. S. Khan, M. S. Awan, S. S. Muhammad, V. Kvicera, M. Grabner, C. Capsoni, E. Leitgeb, and P. Mandl, "Linearity in optical attenuations for free-space optical links in continental fog," Proceedings of the 5th European Conference on Antennas and Propagation, pp. 2504-2507, 2011.

[36] R. Nebuloni and C. Capsoni, "Effect of hydrometeor scattering on optical wave propagation through the atmosphere," in Antennas and Propagation (EUCAP), Proceedings of the 5th European Conference on, pp. 2513-2517,2011

[37] M. Gebhart, E. Leitgeb, S. Sheikh Muhammad, B. Flecker, C. Chlestil, M. Al Naboulsi, F. de Fornel, and H. Sizun, "Measurement of light attenuation in dense fog conditions for fso applications," pp. 58910K-1-58910K-12, 2005

[38] M. Grabner and V. Kvicera, "Fog attenuation dependence on atmospheric visibility at two wavelengths for FSO link planning," in Antennas and Propagation Conference (LAPC), Loughborough, pp. 193-196, 2010

[39] U. Ketprom, S. Jaruwatanadilok, Y. Kuga, A. Ishimaru, and J. Ritcey,"Channel modeling for optical wireless communication through dense fog,"J. Opt. Netw., vol. 4, pp. 291-299, 2005

[40] F. Nadeem, V. Kvicera, M. S. Awan, E. Leitgeb, S. Muhammad, and G.Kandus, "Weather effects on hybrid FSO/RF communication link," Selected Areas in Communications, IEEE Journal on, vol. 27, pp. 1687-1697, 2009

[41] V. J. Schaefer and J. A. Day, "A Field Guide to the Atmosphere",Houghton Mifflin, 1998

[42] H. E. Nistazakis, T. A. Tsiftsis, and G. S. Tombras, "Performance analysis of free-space optical communication systems over atmospheric turbulence channels," Journal of IET Communications, vol. 3, pp. 1402-1409, 2009

[43] M. Cole and K. Kiasaleh, "Signal intensity estimators for free-space optical communications through turbulent atmosphere," IEEE Photonics Technology Letters, vol. 16, pp. 2395-2397, 2004

[44] R. M. Gagliardi and S. Karp, "The optical communication system," in Optical Communications, J. G. Proakis, Ed. New York: John Wiley and Sons, Inc, pp. 1-3, 1995

[45] S.-R. Moon, H.-K. Lee, and C.-H. Lee, "Automatic wavelength control method using Rayleigh backscattering for WDM-PON with tunable

lasers," Conference on Lasers and Electro-Optics (CLEO) 2011, pp. 1-2, 2011

[46] L. Hong and W. Xinmin, "Study of scattering characteristics of atmospheric aerosol particles based on infrared laser," 2011 Symposium on Photonics and Optoelectronics, pp. 1-5, 2011

[47] Z. Zhang, "Quantitative microplasma electron number density measurement by coherent microwave Rayleigh scattering," IEEE Transactions on Plasma Science, vol. 39, pp. 593-595, 2011

[48] A. Jurado-Navas and A. Puerta-Notario, "Generation of correlated scintillations on atmospheric optical communications," IEEE/OSA Journal of Optical Communications and Networking, vol. 1, pp. 452-462, 2009

[49] X. Liu, "Free-space optics optimization models for building sway and atmospheric interference using variable wavelength," IEEE Transactions on Communications, vol. 57, pp. 492-498, 2009

[50] W. O. Popoola, Z. Ghassemlooy, C. G. Lee, and A. C. Boucouvalas,"Scintillation effect on intensity modulated laser communication systems a laboratory demonstration," Optics and Laser Technology, vol. 42, pp. 682-692, 2009

[51] J. Zeller and T. Manzur, "Free-space optical communication at 1.55 m and turbulence measurements in the evaporation layer," pp. 85400C-85400C,2012

[52] J. Yang, Z. Niu, C. Shi, D. Liu, and Z. A. Li, "Microphysics of atmospheric aerosols during winter haze/fog events in nanjing," Journal of Environmental Science, vol. 31, pp. 1425-1431, 2010.235

[53] J. Bendix, "A satellite-based climatology of fog and low-level stratus in-Germany and adjacent areas ", Atmospheric Research vol. 64, pp. 3-18, 2002

[54] N. Blaunstein, S. Arnon, A. Zilberman, and N. Kopeika, "Applied aspects of optical communication and LIDAR," Boca Raton : CRC Press, London, pp. 53-55, 2010

[55] W. Eugster, "Fog Research," Special Issue, Erde, pp. 1-10, 2008

[56] M. Z. Jacobson, "Atmospheric Pollution" History, Science, and Regulation: Cambridge University Press, 2002

[57] C. F. Bohren and D. R. Huffman, "Absorption and scattering of light by small particles " John Wiley and sons, New York, 1983

[58] H. C. Hulst and H. C. Van De Hulst, "Light scattering: by small particles" Dover, 1957

[59] H. Weichel, "Laser beam propagation in the atmosphere.," Bellingham: SPIE Optical Engineering, vol. TT3, pp. 25-39, 1990

[60] J. C. Ricklin, S. M. Hammel, F. D. Eaton, and S. L. Lachinova, "Atmospheric channel effects on free-space laser communication," Journal of Optical and Fiber Communications Research, vol. 3, pp. 111-158, 2006

[61] G. M. Hale and M. R. Querry, "Optical Constants of Water in the 200-nm to 200-m Wavelength Region," Journal of Applied Optics, vol. 12, pp. 555-563, 1973

[62] A. S. Jursa (sci. ed.), "Handbook of Geophysics and the Space Environment",NTIS Doc ADA16700, Air Force Geophysics Laboratory, Hanscom Air Force Base, Massachusetts, 1985

[63] D. R. Bates, Rayleigh Scattering by Air, Planetary Space Science, vol.32, pp. 785790, 1984

[64] H. C. van de Hulst, "Light Scattering by Small Particles", Wiley, New York, 1957. also Dover Publications, January 1, 1982

[65] http://en.wikipedia.org/wiki/Irradiance

[66] Master thesis by Torbjon nesheim Trondheimn 20/12-1998.

[67] http://www.photonicsonline.com/doc/avalanche-photodiodes-theory-and-applications-0001

[68] PCEdu-1 Photon counting fundamental Educator Pack

[69] http://en.wikipedia.org/wiki/Johnson

Chapter 3

Noise Tolerance and Characterization

3.1 Introduction

In this chapter we study the reliability of the PolSK scheme as the modulated signals travel through atmosphere. Atmospheric effect such as fog, smoke and turbulence affect all free space optical links, irrespective of the modulation scheme. ASK scheme are critically affected due to attenuation where as phase modulation normally gets affected by turbulence phenomena. On the other hand polarization get affected by scrambling of the polarization state. Intuition therefore suggests that PolSK is not really a reliable method for free space communication through atmospheric scatters. But we show below by creating atmospheric effects inside the lab, that polarization degradation is not as harmful as expected and information can still be obtained. Majority of modern day communication protocols are based on optical technology, as these technologies offer higher bandwidths, increased signal to noise ratio and difficult to eavesdrop upon. While most of these depend upon optical fiber channels for transmission, there is some interest in free-space modules. Free space communication are effective in areas where fibers are superfluous - such

as on-chip connectivity, or in areas where fibers can not be laid such as between two mobile units or satellite based systems [1]-[6]. On the other hand, Free space optical (FSO) communication almost always demands a line-of-sight setup with no obstructions in between [1, 2, 3]. It is also severely affected by atmospheric effects, such as fog, turbulences, smoke etc. [10, 13, 14, 15, 16].

In addition, while fiber based optical communication normally makes use of amplitude or phase shift keying for incorporating information, FSO systems can also use polarization modulation, which is relatively more robust than phase or amplitude modulation. In particular, polarization shift keying involves measuring state of polarization using a relative intensity measurement on both polarization axis and hence strong attenuation do not affect the measurement. On the other hand, differential scattering from atmospheric particles such as smoke or fog droplets result in change in polarization of the incident light. Since the particle distribution and hence the scattering is random, the polarized light gets depolarized and the information is lost.

In this chapter, we present experimentally verified amount of depolarization noise due to fog and smoke and compare with known theoretical values. There has been several studies involving simulations [22]-[20] but very few experimental studies to substantiate these simulations. In addition, we provide a more practical measurement technique for determining the state of polarization of the light, which involves less number of measurements compared to a full Stokes parameter determination. Although this technique is useful only in the limited context of the polarization modulation communication scheme, it is nevertheless offers easier and speedier measurement. We show that this technique has a significantly higher tolerance for depolarization noise. We perform our experimental with two different method.

3.2 Synchronization method

Our experimental setup is shown in figure 3.1 where computer sends the signal through DAQmx. There are two laser controllers to control VCESL1 we can call L_1 and VCSEL2 as L_2. We are using PBS1 for two different polarized components. Laser L_1 is vertical and Laser L_2 horizontal. We are using PBS2 to separate polarized component, transmission component received by detector D_1 (vertical) and reflection component received by detector D_2 (horizontal). Detector D_1 receives only light from L_1 while D_2 receives light only from L_2. Unless the polarization is spoiled by randomizer. D_3, on the other hand detects light from both L_1 and L_2 and signals from this is used as clock signal for synchronized. Finally we compose the transmitted and received massage independently to compute the bit error rate. Here we estimate the error rate as a function of synchronization the detector. At first we only fix the timings of the transmitter and receiver without any synchronization. Then we try two types of triggers pulse triggers and edge triggers.

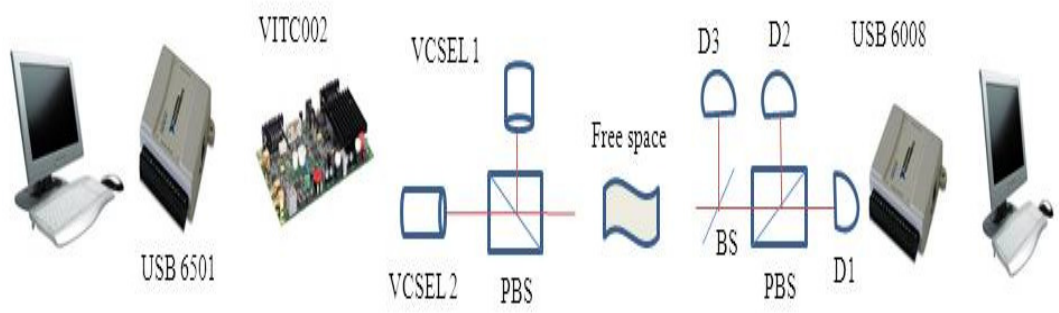


Figure 3.1: Experimental setup

We send 5000 bits without any synchronization between transmitter and receiver shown in fig 3.2. We observed error rate max 50% and bit loss 35%.

Bit received as a function of on time/off time here on time/off time is duty cycle. In fig 3.3 we saw that when we send 499 bit with on time 15ms and off time 15ms which is 0.033 kHz. We received exact 499 bit it means receiver

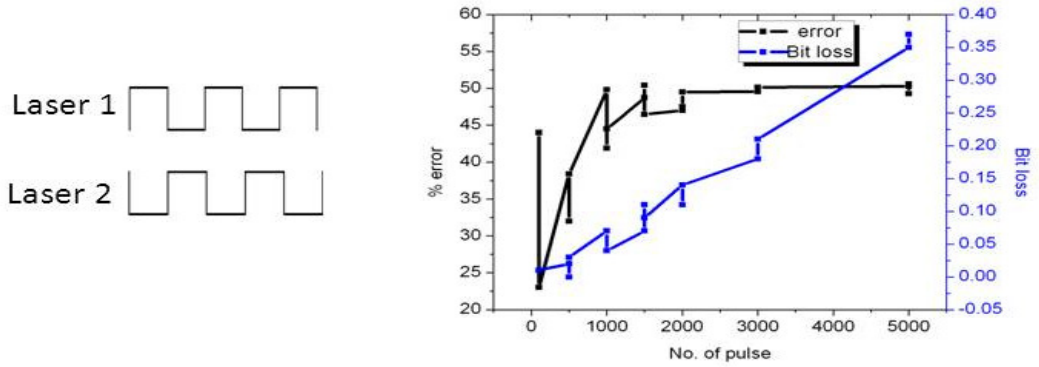


Figure 3.2: Left shows the synchronization sequence of the pulses and right shows the BER as a function of No. of transmitted bit

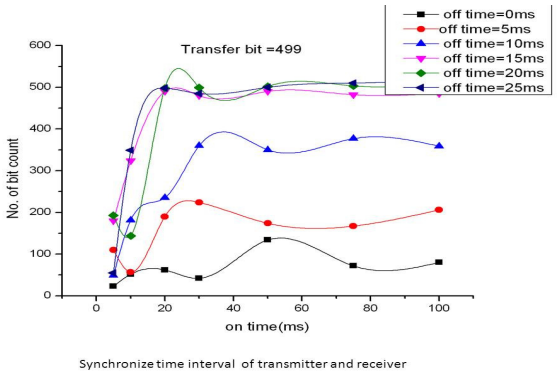


Figure 3.3: Bit synchronization with different frequency

and transmitter are synchronize.

We modified our program and made a delay in clock signal so that the two pulse from L_1 and L_2 have delay. We can see after every pulse there is a delay in clock detector. We synchronize our transmitter and receiver to this clock sequence fig 3.4. We transfer 499 bits every time by varying on time and off time. We adjusted delay in transmitter to obtain optimum signal reception. Here receiver is completely synchronized with clock signal. Means once the clock is on data will be received.

Receiver is now synchronised with rising edge of the clock pulse. This is to avoid multiple poling when clock is on. Fig 3.5 we reduce percentage

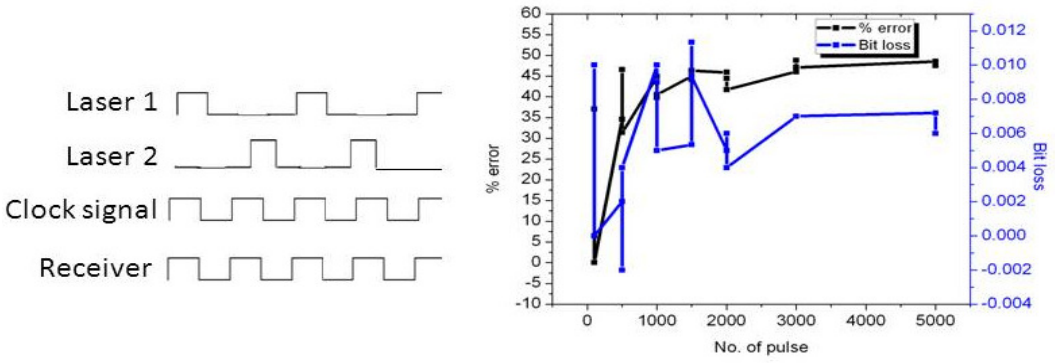


Figure 3.4: Synchronization with clock

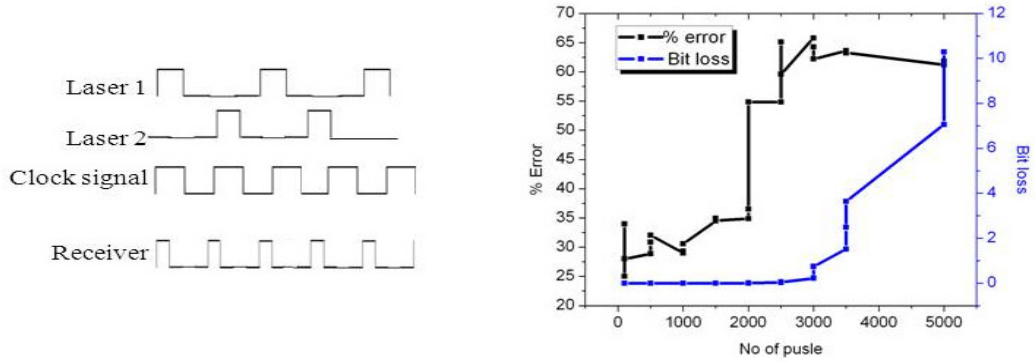


Figure 3.5: Left shows the relationship between various trigger pulses right BER as a function of number of transmitted bit

error but bit loss increased. We observe these method is not reliable to do communication. In next method we changed DAQmx to high frequency and taken electrical pulse as a clock signal.

3.3 Differential polarization method

In this method we present the differential measurement mode. We also shown the detailed experiments involving simulated atmospheric condition in the lab. Using the setup described earlier chapter we investigated the depolarization effect of a simulated atmospheric on the information. We have investigated

effect of fog and smoke and also studied the effect of synchronization of the transmitter and receiver. In this method we proposed a method of differential measurement to determine the polarization of the light pulse at the receiver. We show that this method is more robust and has a high tolerance for depolarization noise by atmosphere. For the sake of completeness, we briefly describe it again as below. Our setup is schematically shown in figure 2.7. The lasers are controlled by a computer using LabVIEW program. Their output beams are mixed into a single channel using a polarizing beam splitter (PBS), such that vertical component from L_1 and horizontal component of L_2 are fed into the main communication channel. L_1 is pulsed when message bit is 0 and L_2 pulse when message bit 1. This ensures that vertically polarized component of L_1 and horizontal component of L_2 is inducted into the communication channel. The receiver consists of another polarizing beam splitter and two Single Photon Counting Modules (SPCM), based on Avalanche Photodiodes (SensL PCDmini 0200 with sensor area 20 μm, cooled to -20° C using Peltier modules). They are labelled APD_1 and APD_2. The TTL pulses from these units are collected using a DAQ card (NI-PCI-6320, from National Instruments) and saved onto the computer using LabVIEW program. In addition both laser pulses and the counting of APD pulses are synchronized to a clock signal. An interference filter with transmission at 780$\pm$2 nm (FL780-10 from Thorlabs Inc.) ensures that stray light from other sources do not enter the detectors. A third laser provides a clock pulse for synchronization of the transmitter and the receiver.

The receiver was now set to count the number of pulses gives by the APD, within the regime of the clock pulse. The SensL APD module comes with two option to take the output of the APD. A built in USB connector to an SMA coupler that gives out TTL pulses for each photon that is incident on the sensor. The output of these module is connected to the counter pins of the DAQ card as explained earlier and a labVIEW code was written to count and record the number of photons thats arrive within the clock pulse. The counts from two APD's are separates records as APD_1 and APD_2, and they indicate

the photon counts of two different polarization. The atmospheric effects are simulated by using a chamber made of glass (35 x 25 x 20 cm) placed in the space between transmitter and the receiver, similar to the setup of Muhammad Ijaz and coworkers [20]. Smoke or fog at various densities are filled into this chamber and the data transmitted through the chamber is analysed. The density of smoke or fog in the path of the communication channel is measured in terms of its effect on the communication, as attenuation of the transmitted light. Since attenuation is proportional to density of scattering particles, higher OD also leads to an increased chance of multiple scattering and hence an increase in number of diffused photons and thus a higher polarization noise. Smoke is created in the chamber by burning household incense powder. Fog is achieved by sprinkling water onto a a sample dry ice kept within. The amount of smoke or fog is quantified by measuring the attenuation of the laser after passing through and characterized by optical density. To characterize the entire system for all possible polarization schemes, a random sequence of ones and zeros were generated by the computer and transmitted. The transmitted and received data are compared to obtain true Bit Erorr Rate (BER). These bit error rates are compared with the theoretical estimate of the BER for normal OOK scheme.

3.4 The concept behind the scheme

Atmospheric phenomena such as fog, smoke etc. are essentially suspended particles in air which scatters the light coming from the transmitter. Most of this light is scattered into random directions and do not reach the detector at all, causing a strong attenuation of the signal. Some part does reach the detector, when multiple scattering events eventually lead it towards the detector (see figure 3.6). However, due to random nature of this scattering, this part of light is completely depolarized. They are referred to as 'diffused' photons. Some lucky photons escape any scattering at all and directly reach

the detector and are termed as 'ballistic' photons. Some more photons suffer minimal, grazing scatterings and reach the detector and are called 'snake' photons. While diffused photons are completely depolarized, snake photons are minimally depolarized and ballistic ones retain their complete polarization [17]. The Degree of Polarization, which is defined by Wolf [18] as the ratio of intensity of polarized component to that of depolarized component, would be equivalent to ratio of number of snake and ballistic photons to number of diffused photons.

Since the information is embedded in polarization of the photons, it is the snake and ballistic photons which are relevant to us. Diffused photons therefore are a part of noise and if more and more of the incident photons fall into the diffused regime, information gets scrambled and will be completely lost. Hence the ratio of ballistic and snake photons to the diffused is equivalent to signal-to-noise ratio, but this quantity depends upon several parameters such as density of scatters as well as scattering cross section etc. A more useful quantity would then be *Degree of Polarization*, which is the ratio of intensity of polarized light to the total intensity, which will be a working definition for signal-to-noise ratio. The atmospheric effects such as fog and smoke cause

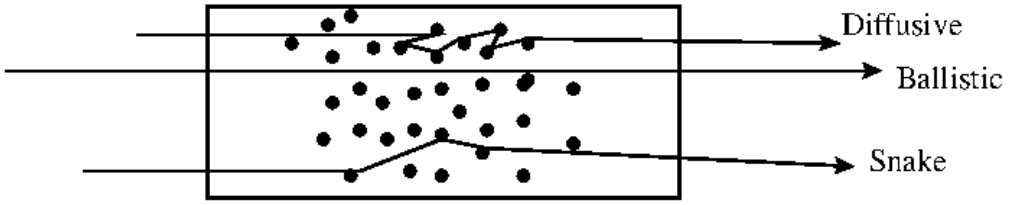


Figure 3.6: Scattering of photons through a multiply scattering media

strong attenuation for free space optical communication. This attenuation critically affects On-Off Keying scheme, resulting in a significant Bit Error rates. On the other hand, phase modulation and polarization modulation schemes are less affected by attenuation, but more affected by differential scattering, which causes random changes in phase and multiple scattering which causes random changes in polarization. Yet, by using comparison measurement tech-

nique instead of measuring absolute polarizations, one can extract information despite a significant amount of polarization scrambling, as shown in following sections. Thus, this scheme has a higher noise tolerance than other schemes.

3.4.1 Degree of polarization and state of polarization

When a purely polarized light becomes partially polarized due to multiple scattering, the correct quantification for such a situation would be a complete four component Stokes Vector $S \equiv \{S_0,\ S_1,\ S_2,\ S_3\}$, which provides a complete representation of the state of the polarization, alongwith the partially polarized nature. However, for a limited use within realm of PolSK, a practical 'State of Polarization' can be defined as SoP $= (I_1 - I_2)/(I_1 + I_2)$, where I_1 and I_2 represent intensities in two orthogonal polarization components. This is a differential measurement and hence will only indicate the normalized difference between the two polarization components. Since information in case of PolSK is represented by any two orthogonal polarization vectors, it is sufficient to know a only a normalized difference between the two, rather than absolute State of Polarization. It will be shown in following paragraphs that this definition allows us to achieve high thresholds for depolarization noise.

If we consider a PolSK involving two linearly polarized lights, vertical and horizontal, mapped to information bits 0 and 1, then the corresponding information mapping would be $1 \sim I_x$ and $0 \sim I_y$. Due to depolarization after passing through the scattering atmosphere, they would respectively become

$$\begin{aligned} I_x &\rightarrow (1-p)I_x + pI_{\text{unpol}} \\ I_y &\rightarrow (1-p)I_y + pI_{\text{unpol}} \end{aligned} \tag{3.1}$$

where p is the depolarization factor, ranging from $p = 0$ for complete retention of polarization and $p = 1$ for a complete depolarization. I_{unpol} is the fraction of original light that has been depolarized. When these two components pass

through the PBS, the respective polarized components would exit appropriate ports of the PBS and reach the respective detectors. But the unpolarised component would split into two equal components, one of which reaches detector APD_1 and the other reaches APD_2. In such a case, for input I_x, the intensity falling on detector APD_1 would be $(1-p)I_x + (p/2)I_{\text{unpol}}$ and APD_2 would receive $(p/2)I_{\text{unpol}}$. Similarly for input I_y, APD_1 would receive $(p/2)I_{\text{unpol}}$ and APD_2 would measure $(1-p)I_y + (p/2)I_{\text{unpol}}$.

The corresponding differential measurement for State of Polarization can be mathematically represented as

$$S = \frac{APD_1 - APD_2}{APD_1 + APD_2} \tag{3.2}$$

For input I_x, it becomes

$$\begin{aligned} S &= \frac{(1-p)I_x + (p/2)I_{\text{unpol}} - (p/2)I_{\text{unpol}}}{(1-p)I_x + (p/2)I_{\text{unpol}} + (p/2)I_{\text{unpol}}} \\ &= \frac{(1-p)I_x}{I_{\text{total}}}, \end{aligned} \tag{3.3}$$

and

$$\begin{aligned} S &= \frac{(p/2)I_{\text{unpol}} - [(1-p)Iy + (p/2)I_{\text{unpol}}]}{(p/2)I_{\text{unpol}} + (1-p)I_y + (p/2)I_{\text{unpol}}} \\ &= -\frac{(1-p)I_y}{I_{\text{Total}}}, \end{aligned} \tag{3.4}$$

for input I_y. I_{Total} is the total intensity, which is sum of polarized and unpolarized components. It can be noted that resultant form of (3.3) and (3.4) turns out to be a slightly modified form of Degree of Polarization as defined by Wolf [18]. While Wolf considers only the absolute value of the above to decipher the amount of light that retains its polarization and neglects its sign,

our differential measurement includes the sign as well which turns out to be useful.

In an ideal case, when there is no depolarization due to scattering, $p = 0$ and hence $S = 1$ for input light of I_x and $S = -1$ for input light of I_y. For a finite value of depolarization, S would provide a value between $[-1, 1]$, from which the input light can be deciphered as being I_x if $S > 0$ or I_y if $S < 0$. It can be noted that unless $p = 1$, which indicates a complete loss of polarization information, the polarization state of input light can be deciphered and the bit mapped to 0 or 1. In this regard, this measurement is much more robust and tolerant to much higher rates of noise. It can be noted that the information is now contained in snake and ballistic photons and the depolarized component of light cancels itself in the differential measurement scheme. Even a small amount of snake and ballistic photons contained in the pulse will be sufficient to mark the information bits to 0 or 1. Figure (3.8) shows result of a typical communication experiment, wherein 50,000 bits were transmitted and SoP was measured for each of them. For each bit a value of SoP was obtained that lay within ± 1. A Histogram of these measurements show a SoP's have a Gaussian distribution, but as long as the distributions of positive and negative SoP values do not overlap, an unambiguous bit value can be assigned.
In the following section, we show an alternate analysis of the same situation, in terms of full Stokes Vector and Müller matrices. The results for the State of Polarization measurement is equivalent to results (3.3) and (3.4).

Traditionally, partially polarized light is described by the Stokes vector $\vec{s} = \{s_0, s_1, s_2, s_3\}$ and a *Degree of Polarization* defined by [18]

$$\mathcal{P} = \frac{(s_1^2 + s_2^2 + s_3^2)}{s_0^2},$$

The value for DOP ranges between 0 and 1, with 0 defining a completely depolarized light and 1 defining a completely polarized light. However, a true evaluation of DOP through stokes vector involves six different measurements. But as long as our information is restricted to two photon states, say vertical

and horizontal, the measurement reduces to two. Some practical definitions can then be obtained as follows.

Consider a horizontal polarized beam denoted by $E_x = \mathcal{E}_x \exp(i\omega t - ik.z)$ and a vertical polarized beam $E_y = \mathcal{E}_y \exp(i\omega t - ik.z)$, with standard notations. After depolarization due to atmospheric scattering, their respective amplitudes can be written as a sum of polarized and unpolarized parts.

$$\begin{aligned} A_x &= \mathcal{E}_x + \mathcal{E}_{unpol} \\ A_y &= \mathcal{E}_y + \mathcal{E}_{unpol} \end{aligned} \tag{3.5}$$

Since polarization is equivalent to information, the unpolarized component represents noise.

We define a 'state-of-polarization' given by

$$\mathcal{S} = \frac{|\mathcal{E}_x|^2 - |\mathcal{E}_y|^2}{|\mathcal{E}_x|^2 + |\mathcal{E}_y|^2}. \tag{3.6}$$

$\mathcal{S}$ ranges from -1 to $+1$ for a purely plane polarized light. The range is less than ± 1 for partially polarized light and the definition can not be used for circular and elliptical polarized light. This is a reduced definition from the full Stokes vector formalism and represents $\{s_1\}$ part alone, which is enough for our purpose.

In the subsequent section, we show that equation 3.6 can be rewritten as

$$\mathcal{S} = \frac{|A_x|^2 - |A_y|^2}{|A_x|^2 + |A_y|^2} = \frac{I_x - I_y}{I_x + I_y}, \tag{3.7}$$

where $I_{x,y}$ indicate the total intensities measured in x and y (Horizontal and Vertical) polarizations. From equation (3.5), it is evident that this term would also include contribution from the depolarized part. However, in our experimental setup, the depolarized part contributes equally to both horizontal and vertical polarized components and hence cancel out in measurement of $\mathcal{S}$, leaving only the contribution from polarized part. This is part is discussed in

detail in following section.

It may be noted that the equation (3.7) is same as the one obtained from the polarization coherence matrix given by Wolf [18], as

$$\mathbf{J} = \frac{1}{N}\begin{bmatrix} \langle E_x E_x \rangle & \langle E_x E_y \rangle \\ \langle E_y E_x \rangle & \langle E_y E_y \rangle \end{bmatrix} = \begin{bmatrix} \rho_{xx} & \rho_{xy} \\ \rho_{yx} & \rho_{yy} \end{bmatrix}$$

where $N = \langle E_x E_x \rangle + \langle E_x E_x \rangle$, is the normalization factor and $\mathcal{S} = Tr(\mathbf{J})$.

3.4.2 Q factor and BER

In traditional On-Off keying system, a Bit Error Rate (BER) is theoretically estimated from the Q factor as [21]

$$\text{BER} = \frac{\text{erfc}(Q\sqrt{2})}{2}. \tag{3.8}$$

However, the PolSK case will have two BER values, each for one polarization, since there are two Quality factors Q_{vertical} and $Q_{\text{horizontal}}$. Even in the traditional On-Off keying, return-to-zero method, the photodiode measurement offers a similar distribution, giving some nonzero value even when the signal is 0. This can be fitted to a Gaussian function [21]. The distribution would then consist of photodiode current when pulse is on (bit 1) and when pulse is off (bit zero). For such situation a Q factor is defined as [19, 21]

$$Q = \frac{I_1 - I_0}{\sigma_1 + \sigma_0}, \tag{3.9}$$

where I_1 is the center for Gaussian for 'on' state and I_0 is the center of Gaussian for 'off' state. σ_1 and σ_0 are the corresponding widths of the Gaussian. However, an equivalent Q factor can not be defined for our case. Since is Q factor is actually a measure of the imperfections, it can be defined as

$$Q_H = \frac{APD_H - APD_V}{\sigma_H + \sigma_V}; \text{ For only Horizontal Transmission}$$

$$Q_V = \frac{APD_V - APD_H}{\sigma_V + \sigma_H}; \text{ For only Vertical Transmission.} \quad (3.10)$$

The values APD_V in first case and APD_H in second case represent leakage and dark count values and corresponding σ_V and σ_H values represent the width of the histograms. Hence the imperfections are accounted for in this measure. Although a perfectly symmetric system with respect to polarization should exhibit equal values for Q_H and Q_V, most commercially available PBS show a little imperfection and hence slightly different values for $Q_{V,H}$. Overall Q factor can be taken as the average of these two.

In the next sections, we describe our results for simulated atmospheric conditions.

The experiment was performed by transferring about 1,00,000 bits of random sequence of 0's and 1's. Smoke was created by burning household incense stick within the glass chamber. Fog was created by spraying water on dry ice. Amount of smoke and fog was quantified by the amount of attenuation caused by it, in terms of optical depth, given by

$$OD = -10 \log_{10} \left(\frac{\text{transmitted light}}{\text{incident light}} \right) \quad (3.11)$$

Individual photon counts from APD_1 and APD_2 are recorded and the State of Polarization, SoP was computed. The information bit was taken to be zero if SoP value was negative and bit was considered 1 if SoP was positive.

When a vertically polarized pulse is incident on the PBS2, only APD_1 should show any counts in ideal case. In reality, APD_2 also shows some counts, which is a sum of dark count of APD_2, change of polarization of incident light due to atmospheric scrambling as well as imperfections of the polarizing

components as well. These counts are obviously counted as noise and a signal-to-noise ratio can be computed. Similarly horizontally polarized light from L_2 results in maximum counts on APD_2 but some 'leakage' is detected on APD_1 as well. A statistical distribution of this phenomena is showed in figure 3.7.

3.5 Stokes vector and Müller matrix analysis for $0^0$and 90^0 polarization based communication

The relevant Stokes Vector and Müller matrices associated with the first PBS, depolarizing field in free space and the second PBS are given as M_1, M_2 and M_3 respectively. Since PBS has two outputs, the corresponding müller matrices are represented by M_i and M_i', with the primed components standing for horizontal and unprimed components indicating outputs at vertical port of PBS. They are given as

$$M_{1,3} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix}.$$

and

$$M_1' = M_3' = \frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

where, a is the depolarization factor. For an ideal case, $a = 1$ for when the state of polarization of input state is preserved and $a = 0$ for a complete depolarization. Comparing with analysis in previous section, we note that a is

same as $1-p$. In this situation, the outputs of polarizing beam splitter (M_3 and M_3') are equivalent to taking projections of the input Stokes vector onto two different states, each of which gives a probability of 0.5.

Net measurement from detectors D_1 and D_2 would then be

$$D_1 = (M_3.M_2.M_1)L_1 + (M_3.M_2.M_1')L_2$$

and

$$D_2 = (M_3'.M_2.M_1)L_1 + (M_3'.M_2.M_1')L_2 \tag{3.12}$$

During communication, either L_1 is on or L_2 is on, with the corresponding Stokes vectors being $L_1 \equiv \{1,1,0,0\}$ and the $L_2 \equiv \{1,-1,0,0\}$. After passing through the PBS as well as the atmosphere, the light falling on detector D_1, when L_1 is on, is given by
D_1=M3M2M1L_1
Where M3 and M1 are PBS muller matrix and M2 is matrix of atmospheric turbulence.

$$D_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{3.13}$$

$$D_1 = \frac{1}{2} \begin{pmatrix} 1+a \\ 1+a \\ 0 \\ 0 \end{pmatrix} \tag{3.14}$$

and the light falling on detector D_2, due to atmospheric depolarization

would be The output of APD_2 when L_1 is on

$$D_2 = M_3'.M_2.M_1.L_1$$

$$D_1 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{3.15}$$

$$D_2 = \begin{pmatrix} 1-a \\ -1+a \\ 0 \\ 0 \end{pmatrix} \tag{3.16}$$

The signal detected by the APD's, after passing through the second PBS would be the $\{S_2\}$ component of the Stokes Vector. Using this component to compute 'State of Polarization' as per equation (3.2), gives us

$$\frac{\{D_2\}_2 - \{D_1\}_2}{\{D_2\}_2 + \{D_1\}_2} = \frac{-1+a-1-a}{-1+a+1+a} = \frac{-1}{a} \tag{3.17}$$

Similarly the output of APD_1 when laser L_2 is on $D_1 = (M_3.M_2.M_1')L_2$

$$D_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \tag{3.18}$$

$$D_1 = \begin{pmatrix} 1-a \\ -1-a \\ 0 \\ 0 \end{pmatrix} \tag{3.19}$$

The output of APD_2 when L_2 is on $D_2 = (M_3'.M_2.M_1')L_2$

$$D_2 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \tag{3.20}$$

$$D_2 = \begin{pmatrix} 1+a \\ -1-a \\ 0 \\ 0 \end{pmatrix} \tag{3.21}$$

$$\frac{\{D_2\}_2 - \{D_1\}_2}{\{D_2\}_2 + \{D_1\}_2} = \frac{-1-a-1+a}{-1-a+1-a} = \frac{1}{a}. \tag{3.22}$$

Equations (3.17) and (3.22) show that the in absence of any atmospheric depolarization, $a = 1$ and the SoP would be ± 1 depending upon whether lasers L_1 or L_2 is on. Depolarization due to atmosphere will give a finite value for a and hence the SoP would decrease. For a a full depolarization, $a = 0$ and hence SoP would be indeterminate. For all other situations, SoP gives a value between $+1$ and -1. It can be inferred from this that if SoP value is negative, then the light contains a vertical polarized component over an unpolarized base and hence the information bit is 0. On the other hand, if the SoP is greater than zero, then it contains a horizontal polarized component over and above a depolarized part and hence the original information is 1. This mapping is very reliable as long as the light is not completely depolarized, as we show below.

3.6 Results & discusssions

We present below the results of our experiments. In order to uniformly test the effect of polarization degradation, we initially create a random sequence of 0's and 1's using the LabVIEW's psuedo-random number generator. The sequence is checked for auto-correlation and cross-correlation and both are

found to be very near 0.5. These random bits are then mapped to L_1 and L_2 and transmitted through free space.

Prior to calculating the SOP, we calibrated our system by first transmitting only vertical or horizontal polarized pulses and noting down the counts at the detector. When only horizontal polarized light is incident, only APD_2 should show counts. But we noticed that APD_1 also has some counts (figures 3.7 APD_1 signal and APD_2 leakage). Similarly, when only vertical polarized pulses are transmitted, APD_2 has some background counts even though only APD_1 should have shown all the counts (figures 3.7 APD_1 leakage and APD_2 signal). These are due to imperfections in polarizing beamsplitters as well as some dark counts of the APDs, which we term as 'leakage'. Despite this, the information is discernible as long as the two histograms of figure 3.7 do not overlap.

We then transmitted the random sequence of 0's and 1's for about 50000 data bits, SOP was computed for each bit using formula 3.2. A histogram of different SOP values were obtained and shown in figure 3.7. It shows two peaks, centered at ± 1 respectively. It also shows that the distributions are not overlapping. In addition, these two peaks were fitted independently to Gaussian functions, in order to obtain the width of these distributions3.9.

The width is a measure of polarization impurity, since pure polarized light should give a very narrow distribution. The impurity is either due to actual degradation of polarization or could also be due to measurement errors and dark counts of the APD's. A very badly degraded polarization, or bad measurement would give rise to overlapping regions of the SOP peaks, indicating areas of erroneous bit assignment.

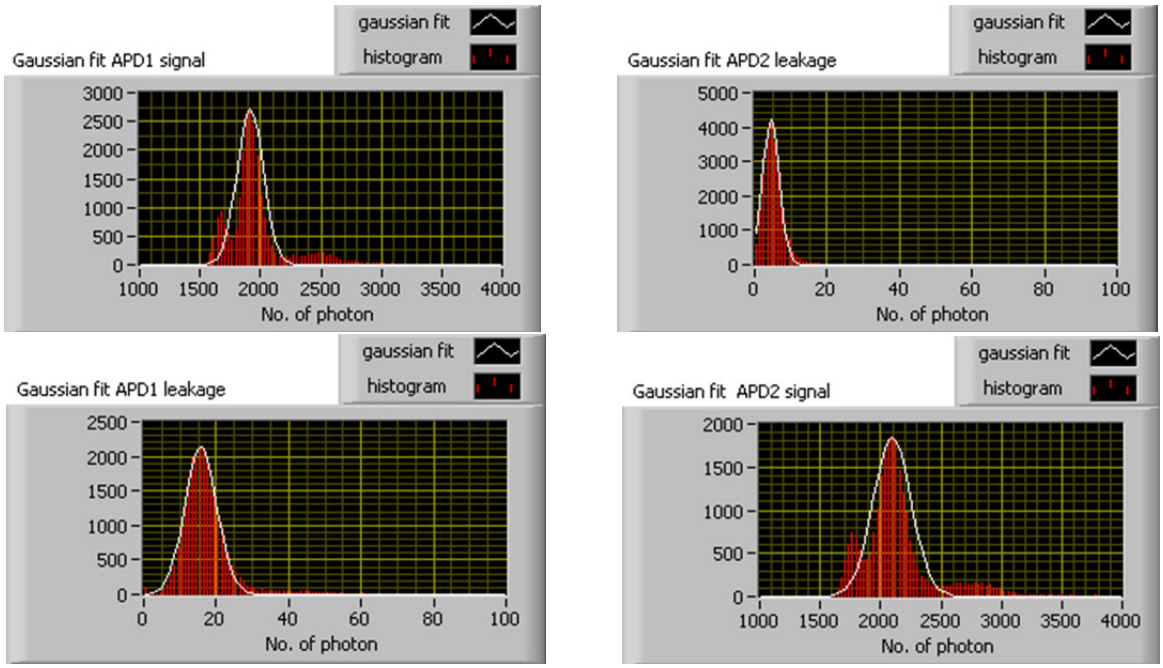


Figure 3.7: Histograms for photon counts for calibration data (a) and (b) are respectively APD_1 and APD_2 counts when only L_1 is used with vertical polarized pulses. While APD_1 alone should have registered counts, APD_2 also exhibits some counts, though averaged at about 15 as against average of 2000 counts for APD_1. Similarly (c) and (d) are for when only L_2 is used (horizontal polarization). This background counts (termed 'leakage') are due to dark counts, stray light as well as some imperfections in polarizing beam splitters. Since histograms do not overalp, signal can be extracted inspite of these imperfections.

3.6.1 Smoke

Smoke was created in the chamber by burning household incense stick inside chamber. This created dense but lightweight smoke particle which hung inside chamber for sufficient time. Different amount of smoke was created by burning the stick for different amount of time, and the amount of smoke was quantified by the optical density, as given by equation 3.11. About 50,000 data bits were transmitted for each bunch and corresponding Q and BER for each polarization was computed.

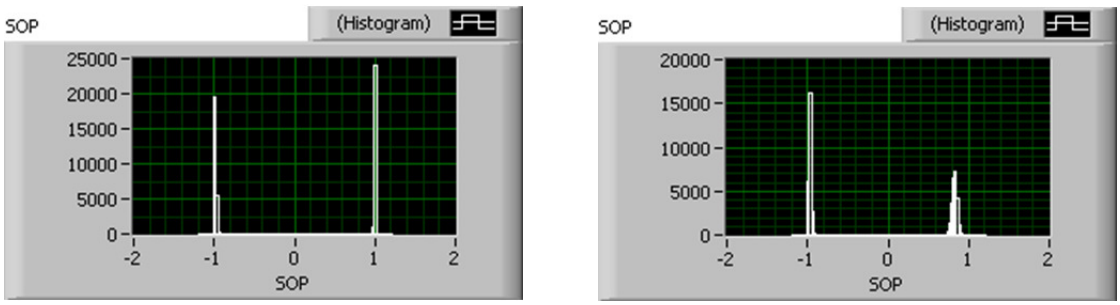


Figure 3.8: (a) Distribution of state of polarization with no atmospheric effects in between. The distribution consists of two non-overlapping peaks centered at -1 and $+1$ respectively. (b) With smoke at OD=-25 dB in path. The range is reduced from ± 1. However, bit assignment will not have errors until the distributions start overlapping.

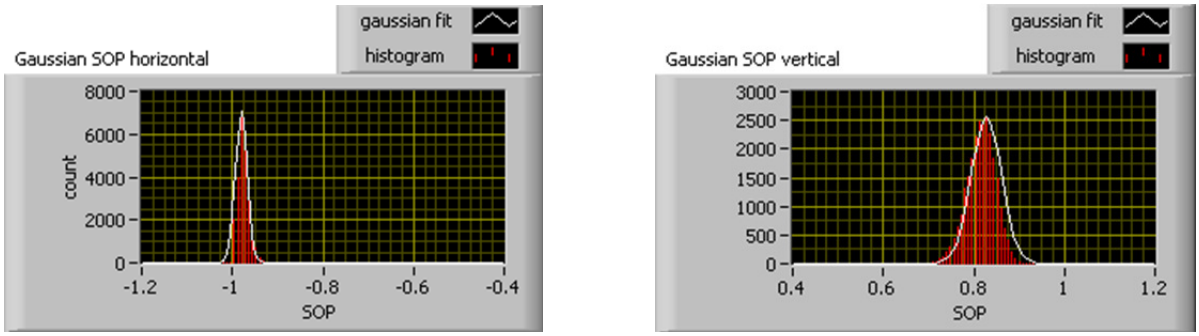


Figure 3.9: Guassian fits for individual peaks

3.6.2 Fog

Fog is an atmospheric condition made up of tiny water droplets, which also scatter light. Attenuation due to scattering, rather than absorption as in case of smoke is the key issue in case of fog. Multiple scattering by fog droplets also degrades polarization. Fog particles are larger than smoke particles and hence scattering cross section is higher. The polarization changes due to scattering is also different from that for smoke.

We created fog in the chamber by sprinkling water over dry ice. As in case of smoke, a random sequence of 50,000 bits were transmitted using two VCSELs

and the SOP for received data was computed. The Q factor and resulting BER were also obtained in similar fashion. Since the scattering characteristics and size distributions are different for fog and smoke, the theoretical Q and BER behaviour are also different. Q reduces at much faster rate and reaches zero even at OD of -10 dB. Theoretical BER, as computed by OOK formula reaches nearly 50% for higher OD's, indicating a complete loss of information.

As in case of smoke, we also calculated BER from comparing actual transmitted and received data. Although in case of smoke, the experimental BER for PolSK was much smaller than the theoretical BER for OOK, fog data on the other hand shows much closer comparison. This is because the scattering loss for polarization are different for smoke and fog particles.

3.6.3 vertical & horizontal polarizations based communication

Figure (3.12) shows Q factor for horizontal and vertical polarized lights in presence of smoke. Optical density as defined by equation (3.11) is used for quantifying the amount of smoke in the chamber. It can be noticed that as Optical density increases from 0 to -30 dB, the quality factor Q reduces to almost zero. This is expected since the multiple scattering by the smoke particles degrades the polarization and errors increase. We fit an exponential curve to fit the data, indicated by thick line and shows a good agreement.

Figure (3.14) shows corresponding bit error rate, as given by equation (3.8). The theoretical BER is almost zero for small OD's but then increases rapidly for higher ODs. reaching almost equal to 25% as optical density increases to -30 dB, which would be a significant amount of scrambling.

As earlier, SOP was computed for each bit. A histogram of the SOP distribution shows that its range is reduced from ± 1 to a lesser range (figure 3.9). However, the distributions are still not overlapping and hence it can be safely assigned to bit 0 when SOP is negative and to bit 1 when SOP is positive. After transmission, each bit on receiver was compared with the

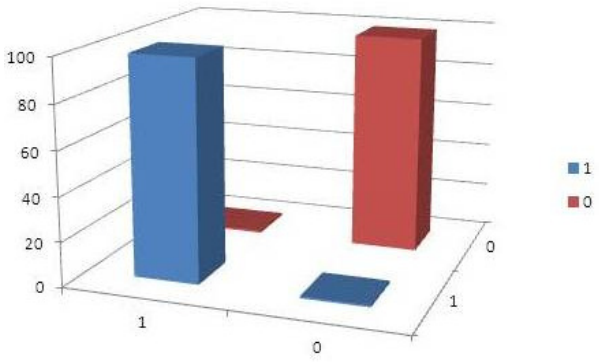


Figure 3.10: Correlation between transmitted bits

transmitted data and correlation between them was computed. The cross-correlation is almost zero and all bits are therefore transmitted with a very high fidelity. Figure 3.10 shows that despite high attenuation of light and a high degradation of the initial polarization, the actual bit error are almost zero and fidelity of transmitted data is very high, as can be seen by $1-1$ and $0-0$ correlations. But at higher concentrations of smoke or fog, errors do develop,

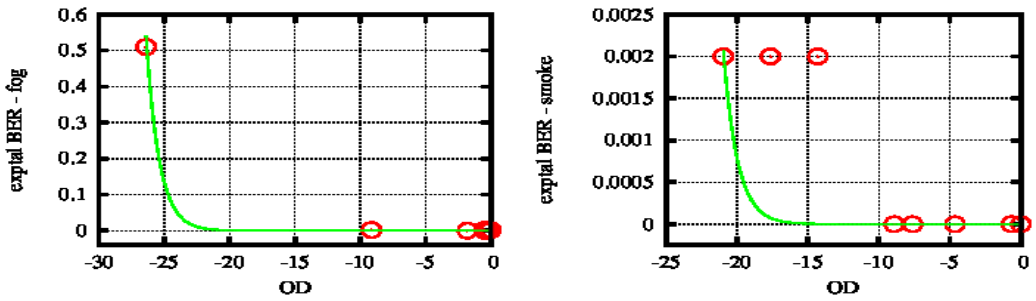


Figure 3.11: Experimentally obtained BER from comparing transmitted and received data in presence of fog (left) and smoke (right). Solid lines are fit for exponential curve.

as shown by figure 3.11. It can be noted that actual BER is nearly zero for a very high amount of smoke, and suddenly increases only at a very high OD, like -30 dB. This shows that despite theoretically low values of Q and high values of BER, the actual BER is very less. It can be noted that theoretical

BER is computed for On/Off keying while the experimental value is for PolSK, indicating that PolSK is much more robust compared to OOK. At very high OD, the error is more due to the very high attenuation wherein the APD's read zero counts rather than due to polarization scrambling.

For each bit at the receiver, the SoP was computed as per equation (3.2). A histogram of the distribution of these SoP values was obtained from which $I_{1,2}$ and $\sigma_{1,2}$ was derived by a curve fit to a Gaussian. From these Q factors and Bit Error Rate values were computed for different smoke/fog conditions. The SoP values were then mapped to actual bit values, which were then compared with the actual transmitted values to obtain the experimental Bit Error Rate. Results of these are given below. The raw data of both Q factors and Bit Error rates were fitted to a stretched exponential function

$$Q = Aexp(x - x_0)^{\beta} + c, \tag{3.23}$$

Here, A is the amplitude, x is the Optical Density, x_0 is the shift in scaling and β is the stretch coefficient. We have analyse our based on erliar define quality factor and bit error rate.

Figures 3.12 show the relevant data for vertical and horizontal polarisations in presence of fog and smoke. It is obvious that the fog and smoke affect the data differently, partly due to the differences in average particle size distributions and also due to different scattering cross sections. Fog particles are likely to be larger than smoke particles but also have different constituents. Fog is suspended water droplets while smoke particles are carbon. In our data, fog shows a rapid decrease in the Q factor, while smoke shows a relatively slower decrease. This is most likely due to the fact that fog particles are larger than that of smoke, but also has to do with different scattering cross sections for different polarizations. The stretch coefficients are also different given by $\beta = 1.0$ for fog data and $\beta = 0.49$ for smoke data. However, despite such a sharp decrease in Q factors, our data is not affected much, as shown later.

The estimated BER values are very close to zero for OD almost upto -20

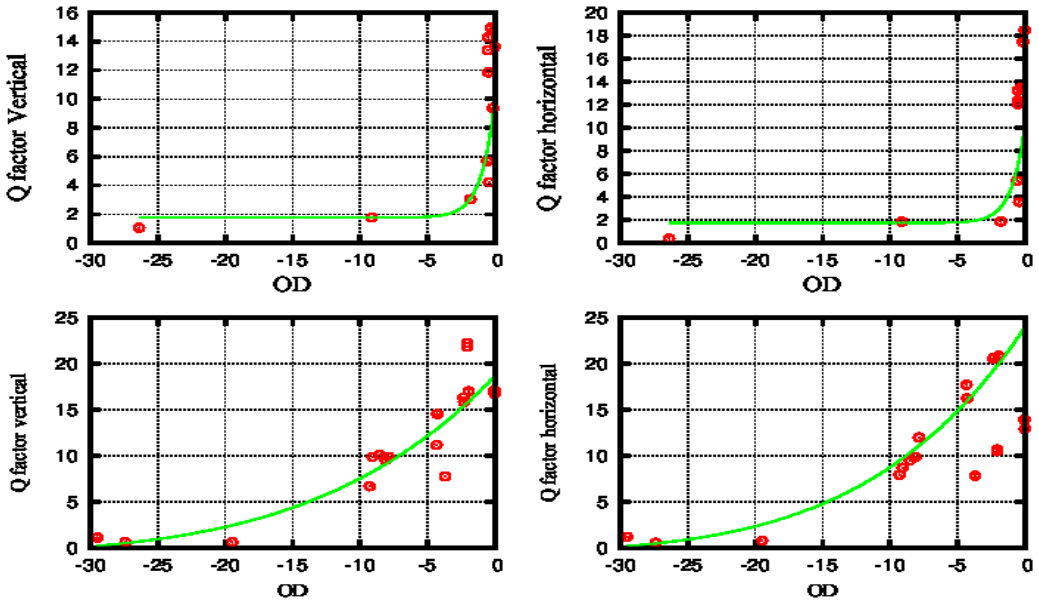


Figure 3.12: Q factors for vertical (left) and horizontal (right), as a function of signal attenuation (a) for fog and (b) for smoke. Solid line is a curve fit for a stretched exponential function. Stretch coefficient $\beta = 1$ for Fog and $\beta \approx 0.5$ for smoke.

dB, after which a sharp rises in BER can be noticed. The actual values of BER, which are obtained by comparing transmitted and received bits are shown in 3.13. These indicate a very similar trend, though the error rates for smoke are much lower than that for fog. This is due to the fact that fog causes a significantly higher depolarization than smoke.

These data are useful in determining a reliability threshold for real communication situation. Since it is impossible to very the actual bit error rates everytime, one can rely instead on the signal attenuation values. When the attenuation values are less than -15 dB, the communication channel can be considered to be very reliable. An attenuation of more than -20 dB would definitely cause depolarization noise leading to a degradation of the signal. In addition, smoke situations are reasonably more reliable than fog situations, even at high attenuation situations.

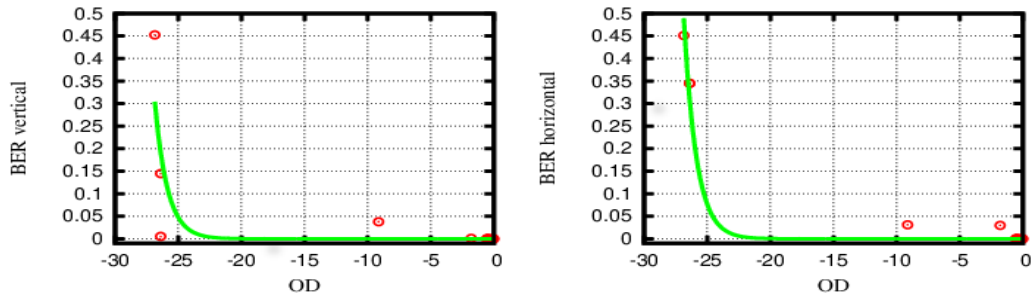


Figure 3.13: Estimated bit error rates for vertical and horizontal polarization, in presence of fog. Solid line indicates an exponential fit with stretch factor $\beta = 1$. BER values are reasonably low for almost upto OD=-20 dB.

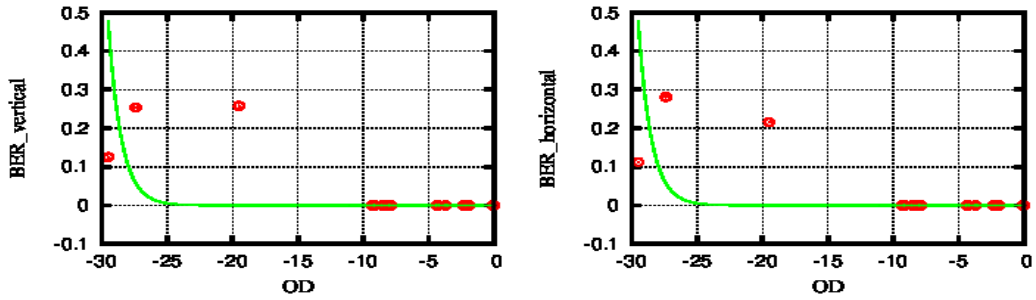


Figure 3.14: Estimated Bit Error rates for vertical and horizontal polarizations, in presence of smoke. Solid line indicates an exponential fit with stretch factor $\beta = 1$. BER values are reasonably low for almost upto OD=-20 dB.

3.7 Conclusions

We have simulated atmospheric conditions inside laboratory to understand noise characteristics in Polarization encoding scheme. We have used vertical and horizontal polarizations to encode message bits. We have also used an Avalanche Photodiode based SPCM to increase sensitivity and work at regime of low incident intensities. Instead of a standard Stokes vector measurement, which requires six different measurements to analyse the state of polarization, we propose a more practical method of using only two measurements, thus reducing the number of detectors and therefore detector noise problems. However, the method proposed works only for horizontal and vertical polarizations and will not work for other modes of polarizations.

We define a State-of-Polarization $\mathcal{S}$ based only two polarization states and show that our method of assigning message bits 0 and 1 to negative and positive values of $\mathcal{S}$ respectively are more practical and show a very low bit error rates even in presence of thick smoke or fog. We compare the bit error for PolSK to analytical bit error rate of OOK scheme and show that PolSK is more robust and lower BER's than OOK, even when theoretical Quality factor is very close to zero.

Although present data is for simulated conditions indoor, the proposed system is easily extendable to outdoor situations. The proposed data analysis is easier requiring much lower resources such as detectors and electronics compared to other schemes.

We have proposed a differential measurement technique to determine bits in case of a polarization modulation scheme. This method measures the snake and ballistic photons, which escape multiple scattering and hence retain their polarization information. The measurement allows us to obtain a SoP value and map negative and positive values to bits 0 and 1 respectively. This method is reliable since unless there is a complete depolarization, which results in a SoP of zero, the bits can be mapped without ambiguity and correctly. Hence the method has a higher noise tolerance and at the same time requires only two measurements hence simpler.

Below a large threshold value of scattering densities, both estimated and measured Bit Error Rates are nearly zero. Beyond this threshold value the BER raises in a very sharp manner. This would be a good technique to prejudge whether or not a communication protocol would be reliable. If a measured Optical densities are above this threshold, the communication is more likely be noisy. If it is less than this threshold, the protocol is likely to be reliable.

In addition, the BER's show an exponential dependency on Optical Density, while the Quality factors show a stretched exponential dependency. In comparison, it is proved by Moeyaert and coworkers [24] that a phase modulation scheme has a stretched exponential behavior for bit error rate. This

aspect of PolSK requires further investigation. The relevance of the stretched exponential would need a more detailed theoretical analysis using monte-carlo methods to simulate polarizing scrambling.

Bibliography

[1] Plank, M. Czaputa, E. Leitgeb, S. S. Muhammad, N. Djaja, B. Hillbrand, P. Mandl, and M. Schonhuber,"Wavelength selection on FSO links," Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP), 2508, 2011

[2] S. A. J. Flörez, "Circular polarization and availability in free space optics (FSO) communication systems", IEEE Latin-American Conference on Communications (LATINCOM 2010), 1, 2010

[3] M. Niu, J. Cheng, and J. F. Holzman, "Diversity reception for coherent free-space optical communications over K-distributed atmospheric turbulence channels," IEEE Wireless Communications and Networking Conference (WCNC 2010), 2010

[4] Fatin Hamimi Mustafa, Abu Sahmah M Supaat, Nachimani Charde, "Effect of Rain Attenuations on Free Space Optic Transmission" International Journal on Advanced Science, Engineering and Information Technology **1** 337 , 2011

[5] W. O. Popoola, "Subcarrier intensity modulated free-space optical communication systems," thesis submitted to University of Northumbria, September 2009, unpublished.

[6] E. Ciaramella, Y. Arimoto, G. Contestabile, M. Presi, A. D'Errico, V. Guarino, and M. Matsumoto, "1.28 terabit/s (32x40 Gbit/s) WDM transmission system for free space optical communications," IEEE Journal on Selected Areas in Communications **27**, 1639, 2009

[7] T. Yamashita, M. Morita, M. Shimizu, D. Eto, K. Shiratama, and S. Murata, "The new tracking control system for free-space optical communications", 2011 International Conference on Space Optical Systems and Applications (ICSOS), 2011

[8] X. Wu, P. Liu, and M. Matsumoto, "A study on atmospheric turbulence effects in full-optical free-space communication systems", 6th International Conference on Wireless Communications Networking and Mobile Computing 2010 (WiCOM), 2010

[9] A. C. Boucouvalas, "Editorial", EURASIP Journal on Wireless Communications and Networking, 2005

[10] E. Dadrasnia, S. Ebrahimzadeh, and F. R. M. Adikan, "Influence of short range free space optical atmospheric attenuation in modulated radio signal," The 2nd International Conference on Computer and Automation Engineering (ICCAE), **5**, 2010

[11] A. Bekkali, C. B. Naila, K. Kazaura, K. Wakamori, and M. Matsumoto, "Transmission analysis of OFDM-based wireless services over turbulent radio-on-FSO links modeled by gamma-gamma distribution", IEEE Photonics Journal, **2**, 510, 2010

[12] N. H. M. Noor, A. W. Naji, and W. Al-Khateeb, "Theoretical analysis of multiple transmitters/receivers on the performance of free space optics (FSO) link", IEEE International Conference on Space Science and Communication, 2011

[13] P. P. Smyth, P. L. Eardley, K. T. Dalton, D. R. Wisely, P. McKee, and D. Wood, "Optical wireless: a prognosis", Proceeding of SPIE, **2601**, 1995

[14] S. A. Zabidi, W. A. Khateeb, M. R. Islam, and A. W. Naji, "Investigating of rain attenuation impact on free space optics propagation in tropical region", 4th International Conference On Mechatronics, 2011

[15] L. C. Andrews, R. L. Phillips, and C. Y. Hopen," Laser Beam Scintillation with Applications", SPIE Press, Washington, 2001

[16] A. K. Majumdar, '"Free Space Laser Communication Performance in the Atmospheric Channel", J. Opt. Fiber. Commun. Rep. **2**, 2005

[17] Hema Ramachandran "Imaging through turbid media", Current Science, **76**, 1999

[18] Wolf E., "Introduction to the Theory of Coherence and Polarization of Light", Cambridge University Press, 2007

[19] M. A. Vorontsov, V. V. Dudorov, M. O. Zyryanova, V. V. Kolosov, and G. A. Filimonov, "Bit Error Rate in Free Space Optical Communication Systems with a Partially Coherent Transmitting Beam", Atmospheric and Oceanic Optics, **26**, 2013

[20] Ijaz M, Ghassemlooy, Z., Le Minh, H. , Rajbhandari, S. , Perez, J. , Gholami, A. "Bit error rate measurement of free space optical communication links under laboratory-controlled fog conditions", 16th European Conference on Networks and Optical Communications (NOC), 2011

[21] John Zweck, Ivan T. Lima Jr, Yu Sun, Aurenice O. Lima, Curtis R. Menyuk, and Gary M. Carter Modeling Receivers in Optical Communication Systems With Polarization Effects, Optics and Photonics News, **14**, 2003

[22] Shalini Khare and Namrata Sahayam, (2012), "Analysis of Free Space Optical Communication System for Different Atmospheric Conditions & Modulation Techniques" Int. J. Mod. Eng. Research, **6**, 4149 - 4152

[23] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, "Quantum Cryptography", Rev. Mod. Phys. **74**, 2002

[24] Moeyaert, V., Mgret, P., Froidure, J. C., Robette, L., & Blondel, M. "Analytical formulation of the error probability of a QPSK transmission impaired by the joint action of gaussian and impulse noise", In Proceedings of the Second IASTED International Conference on Communication Systems and Networks, 2003

Chapter 4

Noise Tolerant M-ary Polarization Encoding in Noisy Atmospheric Channel

4.1 Introduction

In PolSK, information encodes in the polarization angle of electomagnetic radiation called SOP[1]. The modulation based on SOP are called Polarization-shift keying (PolSK) schemes [1, 2, 3]. To transmit bit 'I' ('0'), the polarization angle of the current symbol is shifted by $-\frac{\pi}{4}$ with respect to the previous symbol$\frac{\pi}{4}$ PolSK system is sensitive to polarization fluctuations during its propagation but their phase-noise insensitive property and good performance.

Polarization shift keying (PolSK) systems have been experimentally demonstrated [4] . While the reported experimental demonstrations have been for binary modulation (2-PolSK)[5, 6, 7], detailed analysis of PolSK has been performed for various binary and multilevel (M-PolSK) modulation schemes[8, 9, 1, 10]. The effects of optical amplification [11, 12] and possibilities for coded modulation [13] have also been considered.

In addition to vertical and horizontal polarized light we also tested the

system for $45^0$and 135^0 polarized light. This study is relevant in case of m-ray encoding where in the data can simultaneously be encoded in V/H ($\pm$) as well as $45^0$and 135^0 basis. In standard communication protocols this is equivalant to m-ray encoding practiced in quadurature phase modulation or multiple ASK schemes. At the same time, the newly emerging field of quantum key distribution, as explained earlier, makes use of random $\pm$, x basis selections. Since $\pm$ and x basis are not multiply exclusive and polarizationin one basis can be explained as linear combination in the other basis, it is evident that noise characteristics will have some overlap.

This prompted us to use the some experimental setup and study the effect of atmospheric noise in the x basis as well. Our result shows a significant deviation between two polarization basis.

4.2 Experimental setup

Our setup is schematically shown in figure 4.1. This is the similar setup explained in earlier chapter. Additional part in this setup we introduced a half wave plate after the PBS allows us to choose convert the vertical/horizontal pulses to $45^\circ/135^\circ$ whenever required. This allows us to investigate noise characteristics for vertical/horizontal polarization independently from that for $45^\circ/135^\circ$. The depolarization is different for vertical and horizontal polarization. Since a $45^\circ/135^\circ$ polarization are linear combinations of vertical and horizontal, these would be affected differently from vertical/horizontal aspects.

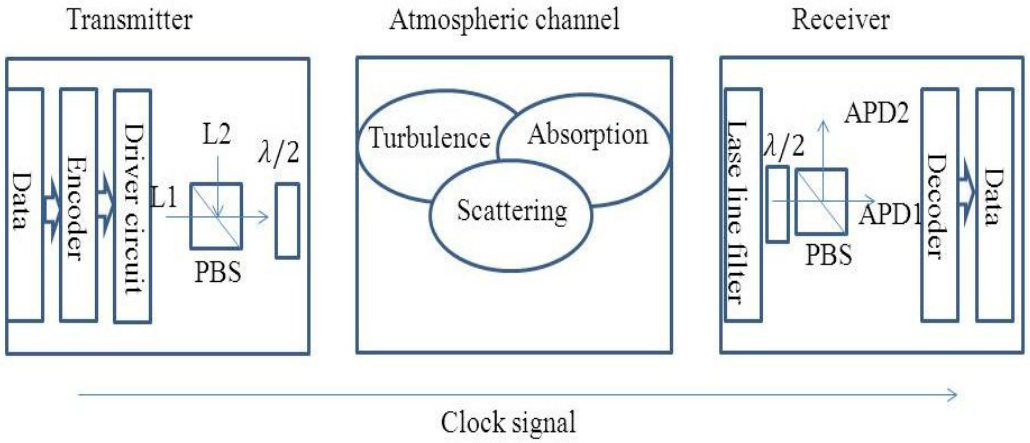


Figure 4.1: Schematic diagram of the experimental setup

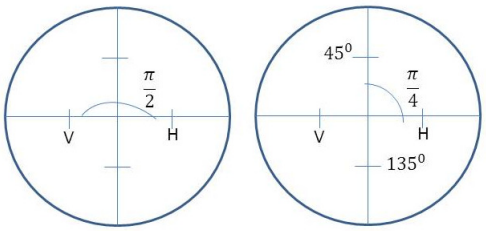


Figure 4.2: Constellation diagram for binary and quarternary PolSK

4.2.1 Stokes vector and Müller matrix analysis for $45^0$and 135^0 polarization based communication

As in case of vertical and horizontal basis, we perform similar calculation for PolSK using 45° and 135° component. we have to add muller matrix for half wave plate.

$$M_4 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

The remaining matrices are same as earlier and we recollect for completeness sake.

$$M_{1,3} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix}.$$

and

$$M_1' = M_3' = \frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$D_1 = (M_3.M_2.M_4)L_1 + (M_3.M_2.M_4)L_2$$

and

$$D_2 = (M_3'.M_2.M_4)L_1 + (M_3'.M_2.M_4)L_2 \tag{4.1}$$

During communication, either L_1 is on or L_2 is on, with the corresponding Stokes vectors being $L_1 \equiv \{1, 0, 1, 0\}$ and the $L_2 \equiv \{1, 0, -1, 0\}$. After passing through the PBS as well as the atmosphere, the light falling on detector D_1, when L_1 is on, is given by

$$D_1 = M_3.M_2.M_4.L_1 = \frac{1}{2}\begin{pmatrix} 1+a \\ 1+a \\ 0 \\ 0 \end{pmatrix} \tag{4.2}$$

and the light falling on detector D_2, due to atmospheric depolarization would

be

$$D_2 = M_3'.M_2.M_4.L_1 = \frac{1}{2}\begin{pmatrix} 1-a \\ -1+a \\ 0 \\ 0 \end{pmatrix} \tag{4.3}$$

The signal detected by the APD's, after passing through the second PBS would be the $\{S_2\}$ component of the Stokes Vector. Using this component to compute 'State of Polarization' as per equation (3.2), gives us

$$\frac{\{D_2\}_2 - \{D_1\}_2}{\{D_2\}_2 + \{D_1\}_2} = \frac{-1+a-1-a}{-1+a+1+a} = \frac{-1}{a} \tag{4.4}$$

Similarly when laser L_2 is on, we get

$$\frac{\{D_2\}_2 - \{D_1\}_2}{\{D_2\}_2 + \{D_1\}_2} = \frac{-1-a-1+a}{-1-a+1-a} = \frac{1}{a}. \tag{4.5}$$

As in the earlier equations (4.4) and (4.5) show that the in absence of any atmospheric depolarization, $a = 1$ and the SoP would be ± 1 depending upon whether lasers L_1 or L_2 is on. Depolarization due to atmosphere will give a finite value for a and hence the SoP would decrease. For a a full depolarization, $a = 0$ and hence SoP would be indeterminate. For all other situations, SoP gives a value between $+1$ and -1. It can be inferred from this that if SoP value is negative, then the light contains a 45^0 polarized component over an unpolarized base and hence the information bit is 0. On the other hand, if the SoP is greater than zero, then it contains a 135^0 polarized component over and above a depolarized part and hence the original information is 1. This mapping is very reliable as long as the light is not completely depolarized, as we show below.

4.2.2 45° & 135° polarizations based communication

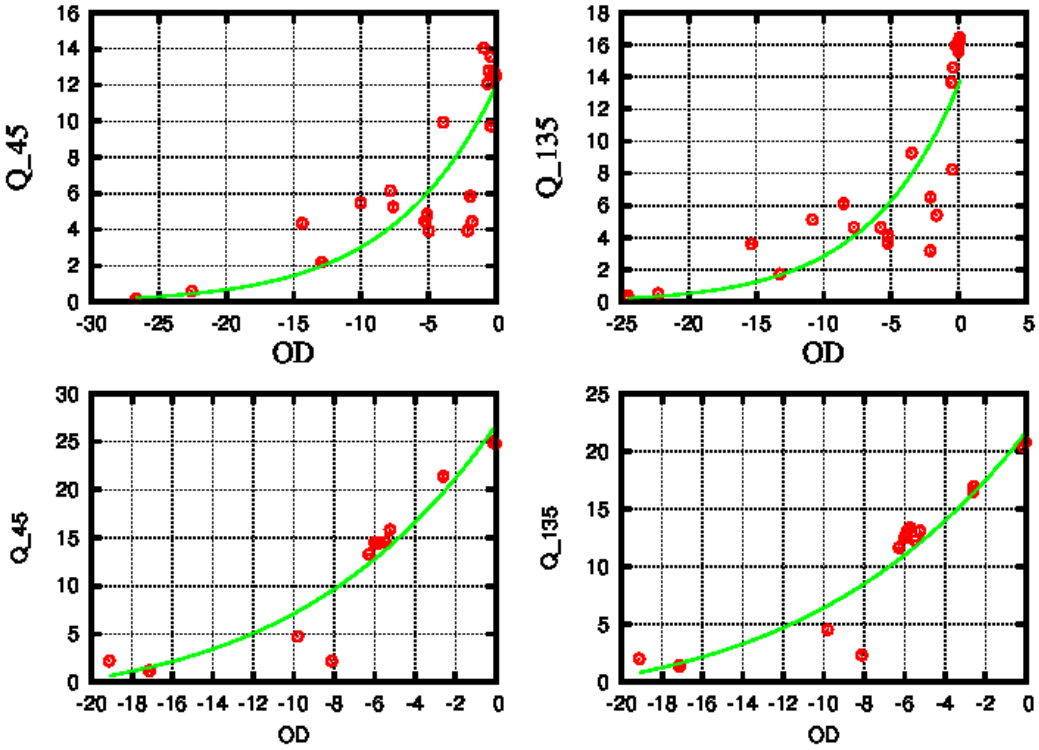


Figure 4.3: Q factor for 45° (left) and 135° (right), as a function of signal attenuation, in presence of (a) fog and (b) Smoke. Solid line is a fit for stretched exponential function. In this case, unlike earlier, both smoke and fog show a trend with stretch coefficient of $\beta = 0.5$

To test transmission of plane polarized light at 45° & 135°, we used halfwave plates with their optical axis positioned at 22.5° to the plane of polarization of incident light. This caused light from L_1 to emerge as 45° polarized light and light from L_2 as 135°, as it enters atmospheric channel. As the earlier case, about 1000 bits per set randomly polarized 45° and 135°were transmitted. The PBS at the receiver is preceded by a half wave plate at 22.5°, due to which the 45° pulse is incident on APD_1 and the 135° pulse is on APD_2

The same labVIEW code now computes the state of polarization and records. After several sets each optical density condition, we compute the

error rate and obtain BER and Q-factor values. They are plotted as a function of OD, as shown in figures 4.3 and 4.4. A curve fitting program is used to obtain best fits for the same functional form

$$Q = Aexp(x - x_0)^{\beta} + c$$

and

$$BER = Bexp(x - x_0)^{\alpha} + c$$

where x represent optical density, α and β are exponential coefficients. The Q factor fits to a stretched exponential with $\beta = 0.5$ while the BER fits to a standard exponential function. However the variation of these quantities with respect to OD is much smother than compared to previous case. The results of Q & BER for the + basis and x basis have significant differences. Although the functional dependency, that is normal exponential of stretched is same, the order of dependency is different. Comparing data in figure 3.12 and figure 4.3, it can be noticed that Q_{45} has a more slow decrease with respect to OD, where as $Q_{vertical}$ has a much sharper drop at about OD=-5. On the other hand in presence of smoke show more or less a similarity slow drop in Q-factor for both situation.Even here, the Q-factor for 45°/135° is relatively slower drop than for V/H.

The bit error rate also shows similar, if not equally drastic diffrencess. A comprasion of figure 4.4 and figure 4.4 shows that $BER_{vertical}$ and $BER_{horizontal}$ are close to zero for almost upto OD=-23dB. On the other hand $BER_{45/135}$ start becoming non zero by around OD=-15dB. In addition, the increse in $BER_{45/135}$ for fog is a smoother than that in case of smoke. This indicates that fog and smoke are more detrimental for 45°/135° than for V/H polarization.

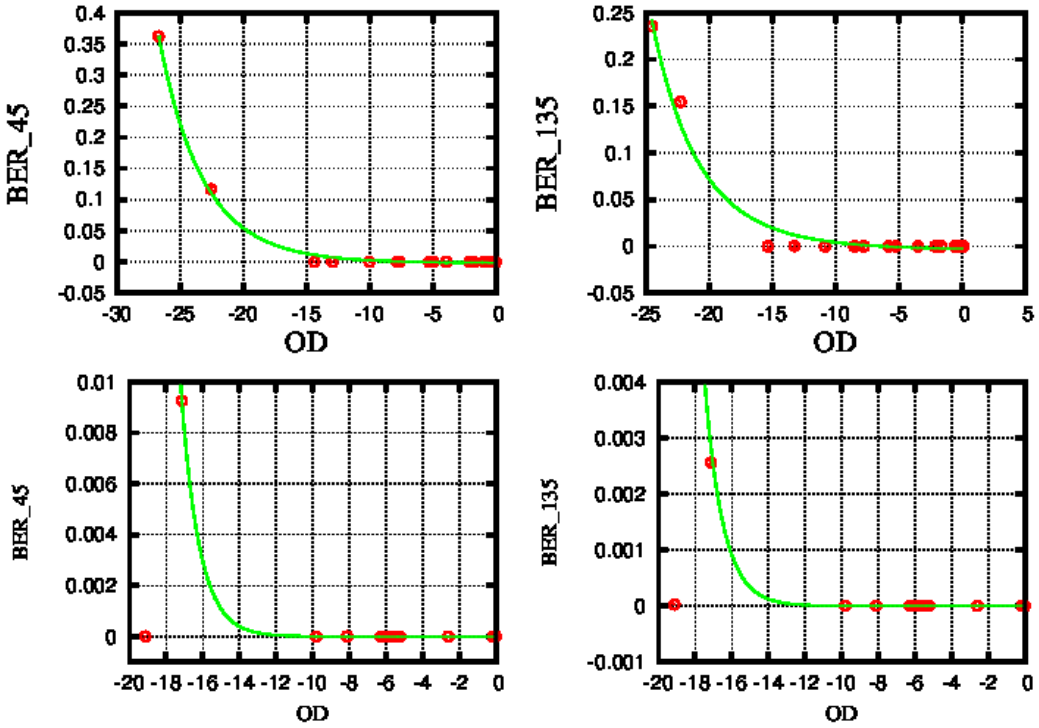


Figure 4.4: BER for 45° (left) and 135° (right), as a function of signal attenuation, in presence of (a) fog and (b) Smoke. Solid line is fit for exponential function. As in case of vertical/horizontal case, BER is close to zero till a threshold value of OD, and increases sharply beyond that. But this increase is much sharper and higher for smoke increases much more than in case of fog.

4.3 Conclusions

In this chapter we have presented the effect of fog and smoke on 45°/135° polarization. we have shown that unlike case of V/H polarization of Q-factor shows a stretched exponential dependency for both fog and smoke. BER fits to normal exponential function for both cases.

This indicate that the decrease in Q-factor and the increase in BER are much smother than in the case for V/H where in they showed a sharp increase/decrease. In addition the noise threshold ratios for the two schemes are different 45°/135° has a threshold of less that -15dB of OD where as V/H exhibit a robustness of more than -23dB. This effect is of concern for both

m-ary encoding as well as QKD schemes. If the atmospheric conditions become noisier that -15dB but less that -23dB, the degradation in information unequal. The information encoded in x basis will be more degraded than that in + basis. At much hgher noise levels, both information will be more or less equally degraded. In other words, the different amount of degradation in each basis needs to be accounted for when using m-ary protocols of QKD protocol that uses polarization encoding.

Bibliography

[1] S. Benedetto and P. Poggiolini, Theory of polarization shift keying modulation, IEEE. Commun., vol.40, no.4,pp. 708-721, Apr. 1992.

[2] S. Betti, F. Curti, B. Daino, G. De Maris, and E. Iannone, State of polarization and phase noise independent coherent optical transmission system based on Stokes parameter detection, Electron. Lett., vol. 24, no. 23, pp. 14601461, Nov. 1988.

[3] C. Jaume, J.M. Gen, J. Prat, IEEE Photon. Technol. Lett. 16 (2004) 1766.

[4] K. Fukuchi, S. Yamazaki, T. Ono, and M. Rangaraj, Polarization shift keyingDirect detection (PolSK-DD) scheme for fiber nonlinear effect insensitive communication system, in Proc. ECOC 92, Sept. 1992, pp.169172.

[5] E. Dietrich, B. Enning, R. Gross, and H. Knupke, Heterodyne trans- mission of a 560 Mbit/s optical signal by means of polarization shift keying, Electron. Lett., vol. 23, no. 8, pp. 421422, Apr. 1987.

[6] R. Calvani, R. Caponi, and F. Cisternino, Polarization phase-shift keying: A coherent transmission technique with differential heterodynedetection, Electron. Lett., vol. 24, no. 10, pp. 642643, May 1988.

[7] S. Benedetto, R. Paoletti, P. Poggiolini, C. Barry, A. Djupsj obacka, and B. Lagerstr om, Coherent and direct-detection polarization modulation system experiments, in Proc. ECOC 94, Sept. 1994, vol. 1, pp. 6771.

[8] S. Betti, F. Curti, G. De Maris, and E. Iannone, Multilevel coherent optical system based on Stokes parameters modulation, J. Lightwave Technol., vol. 8, no. 7, pp. 11271136, July 1990.

[9] S. Betti, G. De Maris, E. Iannone, and P. Lazzaro, Homodyne optical coherent systems based on polarization modulation, J. Lightwave Technol., vol. 9, no. 10, pp. 13141320, Oct. 1991.

[10] S. Benedetto,P. T Poggiolini , Multilevel polarization shift keying: optimum receiver structure and performance evaluation, IEEE Trans. Commun., vol. 42, no. 2/3/4, pp. 11741186, Feb./Mar./Apr. 1994.

[11] S. Betti, G. De Maris, and E. Iannone, Polarization modulated direct detection optical transmission systems, J. Lightwave Technol., vol. 10, no. 12, pp. 19851998, Dec. 1992.

[12] S. Benedetto, R. Gaudino, and P. Poggiolini, Direct detection of optical digital transmission based on polarization shift keying modulation, J. Selected Areas Commun., vol. 13, no. 3, pp. 531542, Apr. 1995.

[13] S. Benedetto, A. Milanesi, G. Olmo, and P. Poggiolini, Applications of trellis coding to coherent optical communications employing polar-ization shift keying modulation, Electron. Lett., vol. 27, no. 12, pp.10611063, June 1991.

Chapter 5

Random Number Generator

5.1 Introduction

One of the key requirement of many cryptograhic schemes is that of random numbers. Sequence of random numbers are used several stages of a standard cryptographic protocol. A simple example is a Vernam cipher, where a string of random numbers is added to massage string to generate encrypted code. $C = M \oplus K$ It has been mathematically shown that this simple scheme is unbreakable if key K as long as M and is used only once. The security of a cryptosystem shall not be based on keeping the algorithm secret but solely on keeping the key secret. The security of a random number generator is related to the difficulty of predicting future values of the sequence from past values. The quality and unpredictability of secret data is critical to securing communication by modern cryptographic techniques. Generation of such data for cryptographic purposes typically requires an unpredictable physical source of random data.

A random process is a repeating process in which output is difficult to find a describable deterministic pattern. The term randomness is quite often used in statistics to signify well defined statistical properties, such as correlation. A variable is random if it follows a given probability distribution.

A good RNG should work efficiently, which means it should be able to produce a large amount of random numbers in a short period of time. Random numbers are widely used in many applications, such as cryptography [1, 2], spread-spectrum communications [3], Monte Carlo numerical simulations [4], and ranging [5] statistical analysis, numerical simulations, information security, stochastic simulation, stream ciphers, encryption codes or keys in digital communication, address codes and spread spectrum codes in code division multiple access (CDMA) and many others. So simulations of random numbers are crucial. Amounts of random numbers are necessary and thus fast RNGs are required. They are also used in the statistics to solve problems in many fields such as nuclear medicine, finance and computer graphics.

Traditional random numbers generated by algorithms are essentially pseudo-random and have potential danger in security-related fields like quantum key distribution. There are in general two types of generators for producing random sequences: true random number generators (TRNGs) and pseudo random number generators (PRNGs). PRNGs need some input called seeds, along with some deterministic algorithms to generate multiple pseudo random numbers. They are usually faster than TRNGs and are preferable when a lot of random-like numbers are required. TRNGs make use of non-deterministic sources along with some post-processing functions for generating randomness. Such sources include physical phenomena such as thermal noise, atmospheric noise, radioactive decay and even coin tossing such as electrical noises [6], frequency jitters in electrical oscillators [7] and chaotic circuits [8, 9], which can produce unpredictable random numbers of high quality yet much lower rates than PRNGs because of the narrow bandwidth of these physical entropy sources. In addition a number of documents exist which provide general advice on using and choosing random number sources [10, 11, 12, 13]. Further discussions on the nature of randomness, pseudo random number generators (PRNGs), and cryptographic randomness are available from a number of sources [14, 25, 16].

A true random numbers is the base of many cryptographical applications such as QKD, especially to generate keys that cannot be penetrated by hack-

ers or other attackers it is important that the random numbers used is unpredictable. The BB84 protocol makes use of polarization states of single photons to map the bits 0, 1 of the encryption key, in two mutually unbiased basis. This results in pulses containing single photons, each randomly polarized. This means that the RNG has to perform better than the Pseudo random number generators (PRNG) available on the computer, but also should be compact and easy to integrate into the prototype QKD device. This requires a controller that generates four random states and its deterministic critically endangers the security of the entire protocol. For most applications it is desirable to have fast random number generators (RNGs) that produce numbers that are as random as possible.

5.2 Random number generator

It is a computational or physical device designed to generate a sequence of number or symbols that lack any pattern, i.e. appear random. In ideal form random number should have following characteristics.

True random number set

- Should be truly random
- Should show no periodicity.
- Not based on an algorithm.
- Should not be predictable based on knowledge of preceding sequences.
- Should not have any hidden correlations

Pseudo random number set

- Pseudo random numbers are good only against computationally limited adversaries
- Although they display qualities of random numbers tests show that there are patterns present
- Subsequent numbers can be guessed

Quasi-random number

- These are a series of numbers satisfying some mathematical random properties even though no random appearance is provided
- They are good for Monte-Carlo methods
- They shows lower discrepancies offer better convergence

5.2.1 Practical use of random number

- They can be used to simulate natural phenomena on a computer useful in many applied disciplines
- Computer programming test program effectiveness test algorithm correctness instead of all possible inputs use a few random numbers Microsoft has used this logic in testing their software
- Decision making, When an "unbiased" decision is needed

5.3 Test for randomness

There are different types of statistical tests that can be applied to a sequence to attempt to compare and evaluate the sequence to a truly random sequence. Some of the standardized tests are Diehard [17], Crypt-XS [18], NIST test suite etc. Random sequence can be characterized and described in terms of probability. In addition, the results of statistical testing must be interpreted with some care and caution to avoid incorrect conclusions about a specific generator.

In this work, we use a set tests designed and implemented by National Institute of Standards and Technology (NIST) test suite is a statistical package consisting of 15 tests [19]. This package will address the problem of evaluating (P)RNGs for randomness. It will be useful in

- Identifying (P)RNG's which produce weak (or patterned) binary sequences.
- Designing new (P)RNG's.
- Verifying that the implementations of (P)RNG's are correct.
- Studying (P)RNG's described in standards.
- Investigating the degree of randomness by currently used (P)RNG's.

The NIST tests focus on a variety of different types of non-randomness that could exist in a sequence. The 15 test are

1. **Frequency test**

   This test determines whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence.

2. **Frequency test within a block**

   This tests whether the frequency of ones in an M-bit block is approximately M/2, as would be expected under an assumption of randomness. For block size M=1, this test degenerates to test 1, the Frequency (Monobit) test.

3. **Runs test**

   This test is to find out if the number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this checks for the oscillation between such zeros and ones as too fast or too slow.

4. **Test for the longest run of ones in a block**

   This one looks for the longest run of ones within M-bit blocks. This test determines whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence.

5. **Binary matrix rank test**

This determines the rank of disjoint sub-matrices of the entire sequence. This test checks for linear dependence among fixed length substrings of the original sequence. This test also appears in the DIEHARD battery of tests [20].

6. **Discrete fourier transform (spectral) test**

This one looks for to detect periodic features (i.e., repetitive patterns that are near each other) in the tested sequence that would indicate a deviation from the assumption of randomness. The intention is to detect whether the number of peaks exceeding the 95 % threshold is significantly different than 5 %.

7. **Non-overlapping template matching test**

This test is to detect generators that produce too many occurrences of a given non-periodic (aperiodic) pattern. M-bit window is used to search for a specific m-bit pattern. If the pattern is not found, the window slides one bit position. If the pattern is found, the window is reset to the bit after the found pattern, and the search resumes.

8. **Overlapping template matching test**

The focus of the Overlapping Template Matching test is the number of occurrences of pre-specified target strings. Both this test and the Non-overlapping Template Matching test use an m-bit window to search for a specific m-bit pattern. If the pattern is not found, the window slides one bit position.

9. **Maurers universal statistical test**

This test is to detect whether or not the sequence can be significantly compressed without loss of information. A significantly compressible sequence is considered to be non-random.

10. **Linear complexity test**

The focus of this test is the length of a linear feedback shift register (LFSR). This test is to determine whether or not the sequence is complex enough to be considered random. Random sequences are characterized by longer LFSRs. An LFSR that is too short implies non-randomness.

11. **Serial test**

This test is to determine whether the number of occurrences of the 2m m-bit overlapping patterns is approximately the same as would be expected for a random sequence. Random sequences have uniformity; that is, every m-bit pattern has the same chance of appearing as every other m-bit pattern. Note that for m = 1, the Serial test is equivalent to the Frequency test[21].

12. **Approximate entropy test**

This test is to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (m and m+1) against the expected result for a random sequence.

13. **Cumulative sums test**

The focus of this test is the maximal excursion (from zero) of the random walk defined by the cumulative sum of adjusted (-1, +1) digits in the sequence. This test is to determine whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behavior of that cumulative sum for random sequences. This cumulative sum may be considered as a random walk. For a random sequence, the excursions of the random walk should be near zero. For certain types of non-random sequences, the excursions of this random walk from zero will be large.

14. **Random excursions test**

This test is to determine if the number of visits to a particular state within a cycle deviates from what one would expect for a random sequence. This test is actually a series of eight tests (and conclusions), one test and conclusion for each of the states: -4, -3, -2, -1 and +1, +2, +3, +4.[22]

15. **Random excursions variant test**

This test is to detect deviations from the expected number of visits to various states in the random walk. This test is actually a series of eighteen tests (and conclusions), one test and conclusion for each of the states: -9, -8, ..., -1 and +1, +2, ..., +9. [23]

5.3.1 P-value

The NIST test suite for characterized the random data by its P-value. The way in which P-value is calculated depend on the nature of test. The P-value

is frequently called the "tail probability". If a P-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A P-value of zero indicates that the sequence appears to be completely non-random. A significance level (α) can be chosen for the tests. If $P - value \geq \alpha$, then the null hypothesis is accepted; i.e., the sequence appears to be random. If $P - value < \alpha$, then the null hypothesis is rejected; i.e., the sequence appears to be non-random. The parameter α denotes the probability of the Type I error. Typically, α is chosen in the range [0.001, 0.01].

An α of 0.001 indicates that one would expect one sequence in 1000 sequences to be rejected by the test if the sequence was random. For a $P - value \geq 0.001$, a sequence would be considered to be random with a confidence of 99.9%. For a $P - value < 0.001$, a sequence would be considered to be non- random with a confidence of 99.9%.

5.4 Generation of random number

We studied three different methods to generate random numbers, which are

1. Chaos based hardware generator
2. Dark Counts from Avalanche Photo Diode
3. Pseudo Random code of LabVIEW

In all these methods we show the efficiency of random number generator by analyzing their statistics.

5.5 Chaos based hardware random number generator

Generally a hardware random number generator is based on sampling noise sources such as thermal noise or reverse based diode. Different circuits are

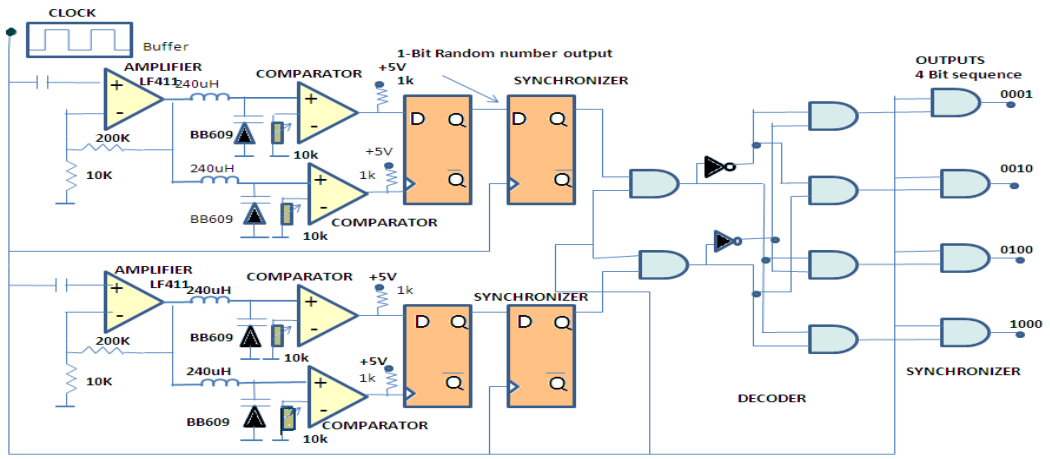


Figure 5.1: Circuit diagram

described in but these methods are difficult since there amplitudes are usually small and often masked by deterministic disturbances so the other alternative is to use a chaotic oscillator for pseudo random generator due to its unpredictable behavior and relatively simple.

We have built a chaotic circuit based RNG (CCRNG), based on an earlier design by T.Kuusela [24]. A simple LCR circuit built around a varactor diode has been shown to behave a chaotic circuit.

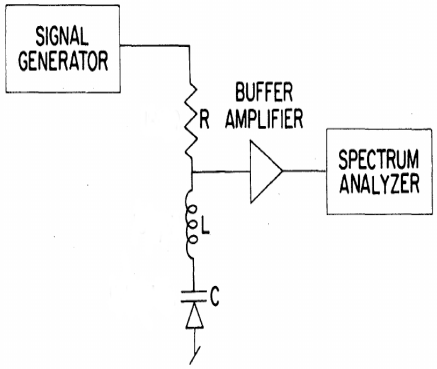


Figure 5.2: Experimental apparatus for sub-harmonic generation

These chaotic circuits are extremely simple consisting of an inductor and a capacitor diode the nonlinear element is the capacitor whose capacitance varied

as a function of voltage across it[25]. The nonlinear capacitance of the diode is seen earlier in many papers. The capacitance is varied as $C(V) = C/(1+V/\theta)\gamma$ where V is the voltage across the diode. If the circuit parameters and the external drive are suitably chosen, the system exhibits period doubling and chaotic behavior.

T. Kussela built a discriminator at the output of this such that it can give a logic bit 1 if the output exceeded a threshold of logic 0 if it was below. The output creates a random sequence of 0's an1's. This circuit was synchronized to a clock input. We added a latch circuit at the end to ensure that the random sequence of 0's and 1's are exactly matching the edge of the clock. This final circuit shown in figure 5.1. It has an external clock signal (A square wave of 500-600 KHz is used as a clock in this case). The CCG includes two identical chaotic oscillators it consists of an inductor 240μH and a varactor diode BB609 (nonlinear element). We are using two CCRNG to generate a sequence of four bit structure in a random fashion, viz., 0001, 0010, 0100 and 1000. Amplifier is used to raise the signal level so that if the frequency and the amplitude of the driving clock is properly chosen the circuit goes to chaotic state and a reliable operation is guaranteed even the case of large tolerance. The fast operational amplifier with a large bandwidth is used as an amplifier (LF 411 is used because of its high bandwidth and fast response). The voltage across the capacitor diode is a random signal when the circuit exhibits period doubling and chaotic behavior. Comparator is used to convert analog signal into a digital signal (LM 311 response time is 200ns). Even though the output of the comparators are quite random to generate it does not generate all the possible bit sequences to all possible values we use two comparators for each CCRNG one of them takes bit sample from the other this is done by a simple D-flip flop(1st D-flip flop). To synchronize the output bit sequences with the driven clock one more D-flip flop is used and a AND gate is used to avoid continues 1s and 0s. A decoder is used to generate four bits structures using two CCRNGs.

Using this circuit we generate several sets of random sequence of 0's and

1's and tested its behavior. At first we tapped the voltage at the output of the chaotic circuit, at the edge of the varactor. This data stored onto the computer as a function of time and then computed its variation dV/dt. Plotting dV/dt against V gives a phase plot. Figure 5.3 showing behavior of the generated signal.

The plot on left side shown the raw data of voltage v/s time at the output of varactor. Plots on the right computed phase plot showing the phase plotdV/dt vs V. The clock frequency is changed in the increasing order form (A) down to (E). In the graph (A) and (B) the clock frequency is less than 500kHz. At this stage the phase plot shows either a constant value. As the frequency is increased the varactor circuit shows a clear bifurcation as in (C). This is the indication of transition towards chaos. At around 650kHz the circuit become complete chaotic, as shown in figure (E). The output of varactor is fed in to the comprator which maps the signal to 1 if the voltage is above a certain threshold and to 0 if it is a below the threshold. The sequence of 0's and 1's generated by the comprator, after synchronized to the clock pulse are recorded on to the computer and analyzed. these data are obtained at the clock speed of about 650 kHz, since this is the region when chaos circuit is giving a proper chaotic output.

Figure 5.4 shows two types of distribution. The total number of 1's and 0's are shown in left side. For this run, there is a asymmetric since there is more 1's than 0. This happen only for few run and can easily be corrected by changing the threshold. The graph on right is more important, since it tells the probability of getting zero following 1, getting a 1 after 1 and simply of 0 after 0 and 1 after 0. the graph shown a slight higher value of occurrence of 11 but this is due to fact that there are more occurrence of 1's as proposed to zero. But the graph clearly shown same frequency for 10 and 01. This means that the system does not have any performance for 1 over 0.

In addition, we studied the bit correlation figure 5.5 of the data at different levels that is $c_{ij}^{00} =< P_i(0)P_j(0) >$ where $P_i(0) and P_j(0)$ are the probability of finding 0 at i^{th} position and j^{th} position respectively. Extending this calcula-

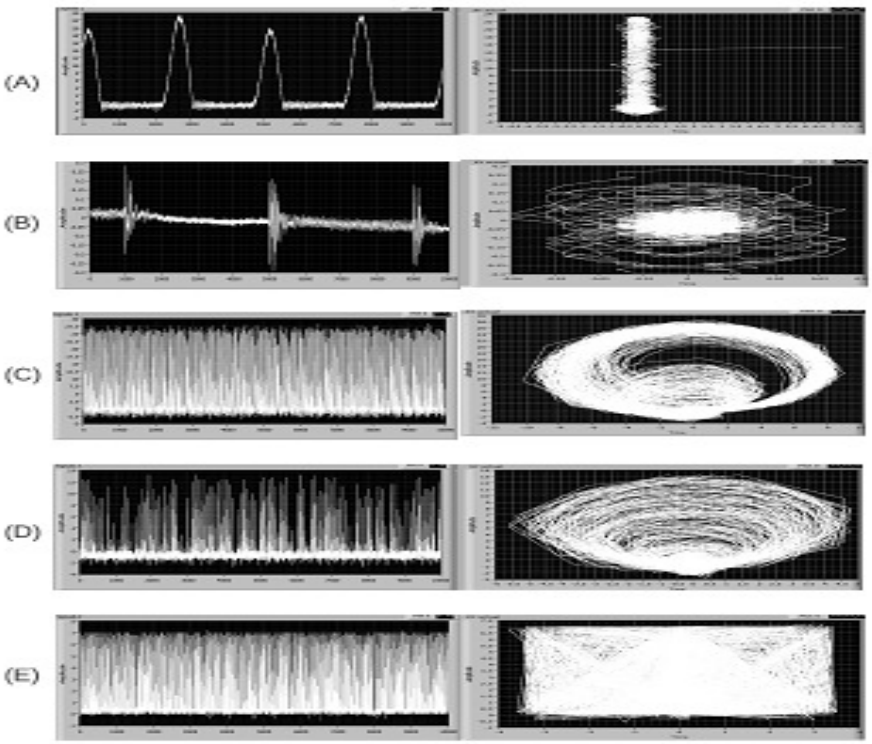


Figure 5.3: Analog signal output of the Chaos Clock Generator at different frequencies and corresponding Phase plots

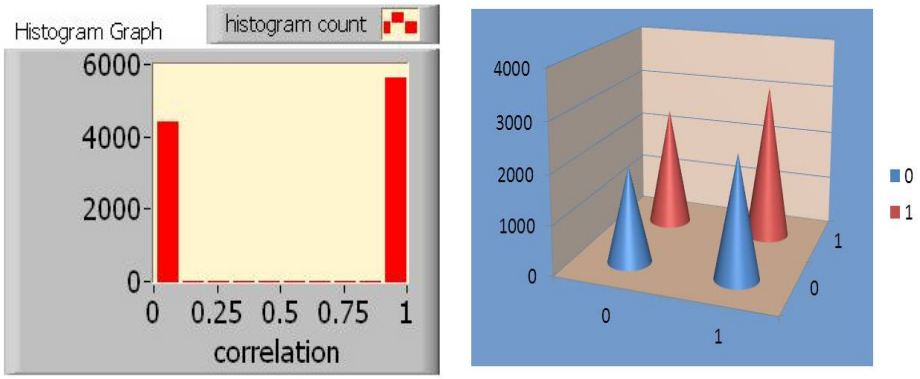


Figure 5.4: Histogram distribution of 0 and 1 (b) bit correlation

tion, we can write $c_{ij}^{kl} =< P_i(k)P_j(l) >$ for k=1,0 and l=1,0. For an ideal case all this should be equal and equal to a value 0.25.

However, figure 5.5 shows that $c_{ij}^{11} = 0.35$ and $c_{ij}^{00} = 0.9$ where as $c_{ij}^{10} =$

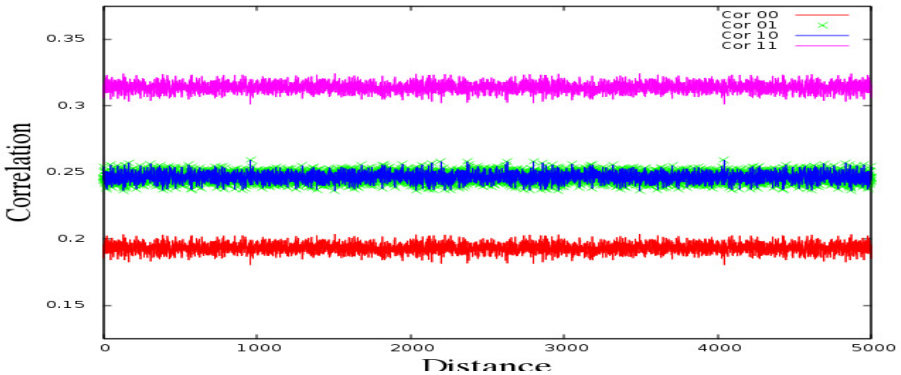


Figure 5.5: Successive bit correlation

$c_{ij}^{01} = 0.25$. This discrepancy in again due to the fact that the circuit is slightly biased towards 1, which is also due to the setting on the discriminator. On the other hand the correlation between 01 and 10 are both equal to 0.25. This indicates the circuit is near perfect coin toss system.

It can be noticed from figure 5.5 bit correlation that the correlation has a small distribution around a mean value. In order to investigate this we plotted the histogram of the bit correlation values. These distribution are shown in figure 5.6. It can be noticed that the distribution of the correlation is very narrow about their mean value.

NIST test

We tested the output of the CRNG circuit using the NIST test suite. For some of the tests the P-value is very small, although some of the other test shows a higher P-value indicating a randomness. Since all the tests are not passed, this is not a very good candidate for randomness. But the resulting correlation indicates that it can be tweaked to obtain a good random number series. We can see from above table maximum cases p-value is zero means is non random. We can not use this number for secure encryption.

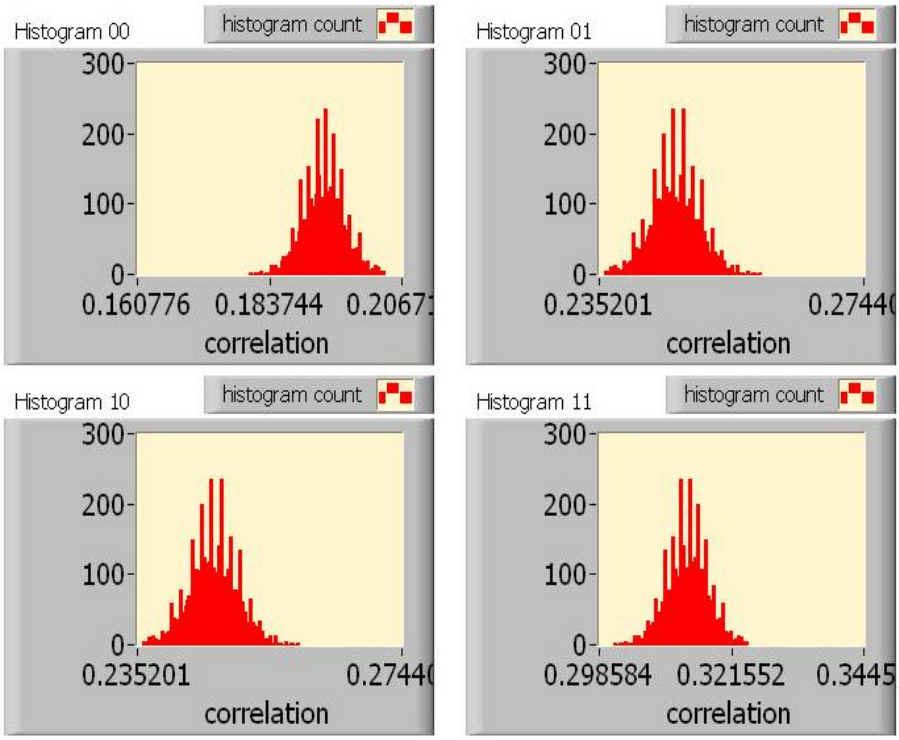


Figure 5.6: Histogram distribution probable finding pair of 00,01,10,11

Statistical test	**P-value**
Frequency	0.000199
BlockFrequency	0.000003
CumulativeSums	0.000439
CumulativeSums	0.017912
Runs	0.350485
LongestRun	0.066882
Rank	0
FFT	0.017912
NonOverlappingTemplate	0.004301
NonOverlappingTemplate	0.002043
NonOverlappingTemplate	0.350485
NonOverlappingTemplate	0.035174

Table 5.1: Result for P-value and passing sequence

5.6 Random number using APD

Our second source of random number generator was the avalanche photo detector. sensL PCDMini is a integrated photon counting device that sensing performance exceeds typical photo multiplier tubes (PMT) values for key photon counting parameters such as photon detection probability, dark counts, timing-jitter and after pulsing. It has included USB interface board integrated into the module which enables the detectors count rate to be easily monitored with the SensL. We have checked its dark count shows Gaussian distribution.

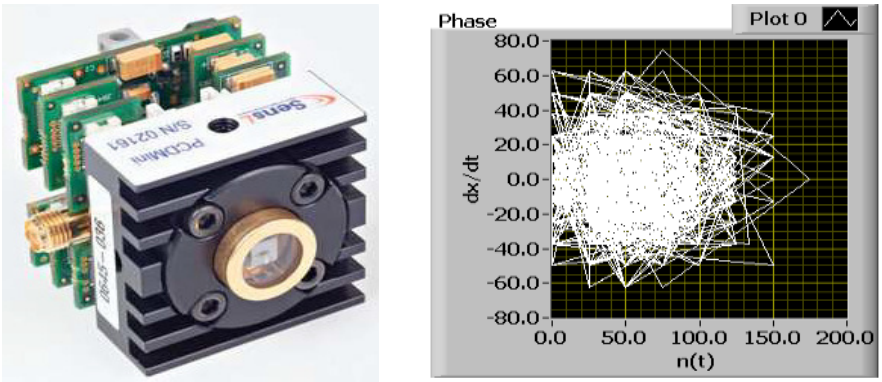


Figure 5.7: (a)Integrated APD device (b)Phase diagram of random output from APD

Figure 5.7 (b) phase plot shows a highly non periodic behavior which is clear indication of randomness. These dark count were converted in to 0 and 1. Figure 5.8 shows two types of distribution. The total number of 1's and 0's are shown in left side. For this run, there is a asymmetric since there is more 1's than 0. This happen only for few run and can easily be corrected by changing the threshold. The graph on right is more important , since it tells the probability of getting zero following 1, getting a 1 after 1 and simply of 0 after 0 and 1 after 0. the graph shown a slight higher value of occurrence of 11 but this is due to fact that there are more occurrence of 1's as proposed to zero. But the graph clearly shown same frequency for 10 and 01. This means that the system does not have any preference over 1 or 0.

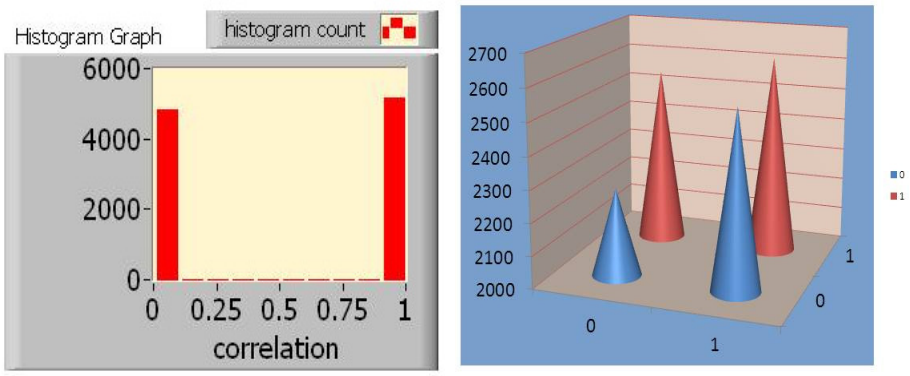


Figure 5.8: Histogram distribution of 0 and 1 (b) bit correlation

We studied the bit correlation figure 5.9 of the data in same fashion as mention above.

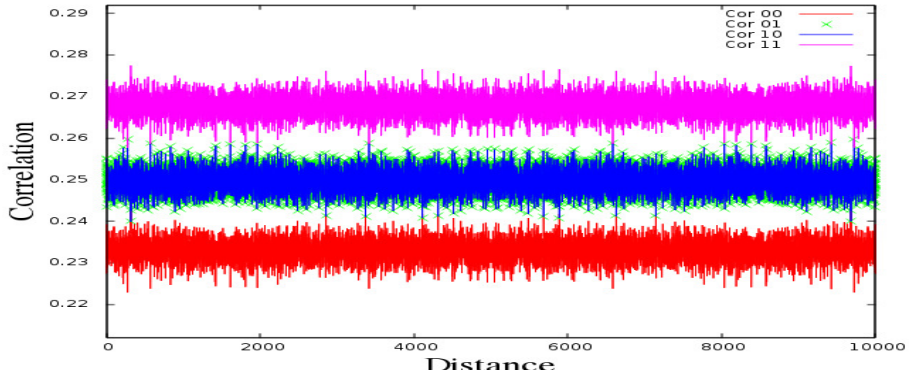


Figure 5.9: Successive bit correlation

Figure 5.9 shows that $c_{ij}^{11} = 0.27$ and $c_{ij}^{00} = 0.23$ where as $c_{ij}^{10} = c_{ij}^{01} = 0.25$. This discrepancy in again due to the fact that the circuit is slightly biased towards 1, which is also due to the setting on the discriminator. On the other hand the correlation between 01 and 10 are both equal to 0.25. This indicates the circuit is near perfect coin toss system.

It can be noticed from figure 5.9 that the correlation has a small distribution around a mean value. In order to investigate this we plotted the histogram of the bit correlation values. These distribution are shown in figure 5.10. It can be noticed that the distribution of the correlation is very narrow about their mean value.

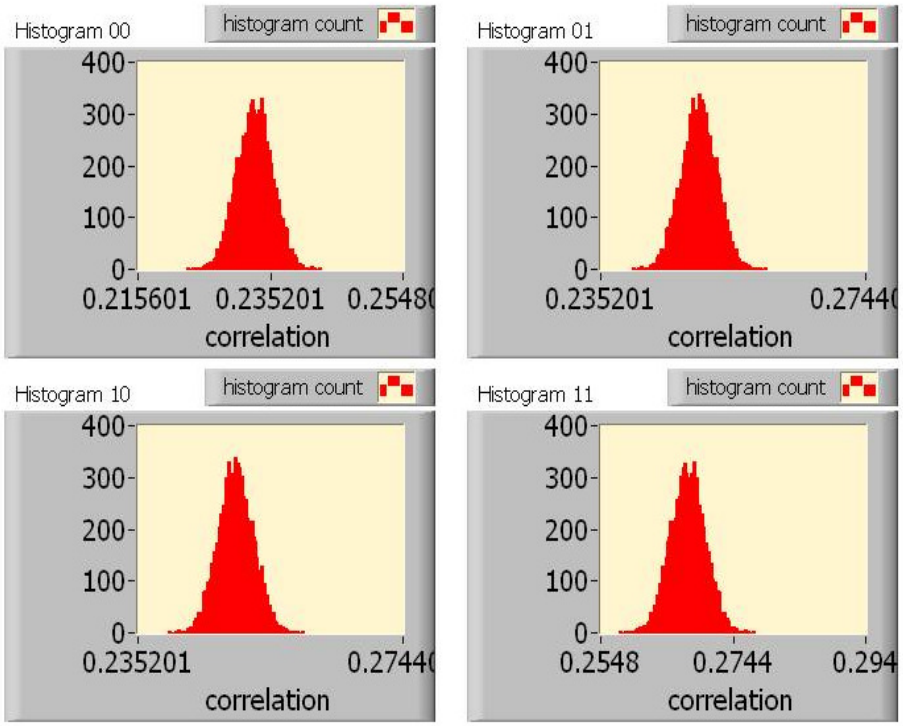


Figure 5.10: Histogram distribution probable finding pair of 00,01,10,11

NIST test

In addition to the correlation test we collected a bit stream of 0's and 1's from the circuit and process through NIST test suite. The result are as

In table 5.2 some of test shows randomness but maximum are showing non randomness behavior.

Statistical test	P-value
Frequency	0.017912
BlockFrequency	0.739918
CumulativeSums	0.213309
CumulativeSums	0.122325
Runs	0.008879
LongestRun	0.350485
Rank	0
FFT	0.534146
NonOverlappingTemplate	0.004301
NonOverlappingTemplate	0.017912
NonOverlappingTemplate	0.035174
NonOverlappingTemplate	0.000001

Table 5.2: Result for P-value and passing sequence

5.7 Random number using LabVIEW

LabVIEW Produces a double precision, floating-point number between 0 and 1, exclusively. The distribution is uniform. We have plotted $\frac{dn}{dt}$ v/s n figure 5.11shows that $\frac{dn}{dt}$ is highly non periodic behavior which is clear indication of randomness. Figure 5.11 is a phase plot shows a highly non periodic behavior

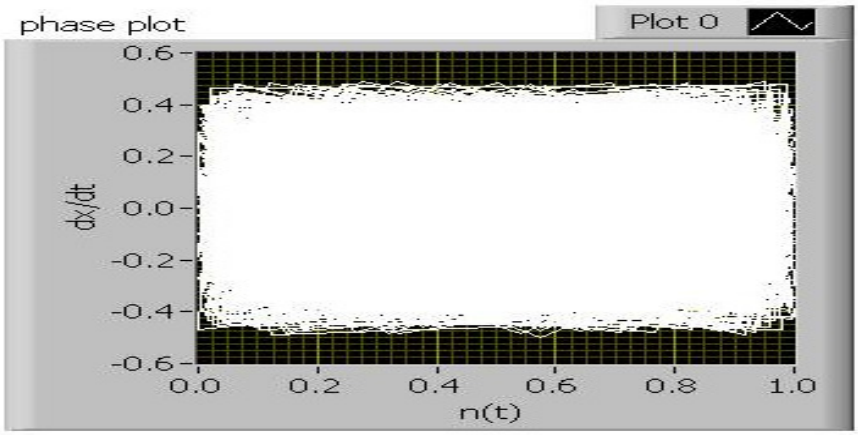


Figure 5.11: Phase plots

which is clear indication of randomness.

The figure 5.12 (a) is histogram graph which is a specific visual representation of data that measures the number of incidents of 0 and 1 of a sample set. left side shown the distribution of 1's and 0's. We observe same frequency for 1's and 0's which is true randomness behavior. The graph on right is more important, since it tells the probability of getting zero following 1, getting a 1 after 1 and simply of 0 after 0 and 1 after 0. the graph shown a slight higher value of occurrence of 11 but this is due to fact that there are more occurrence of 1's as proposed to zero. But the graph clearly shown same frequency for 10 and 01. This means that the system does not have any performance for 1 over 0.

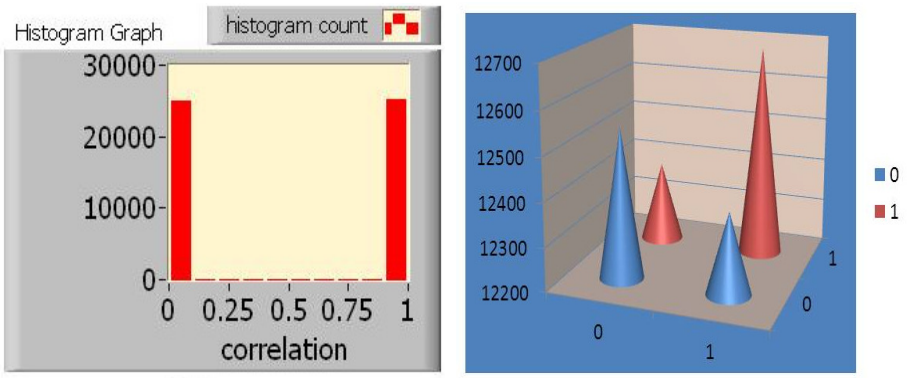


Figure 5.12: Histogram distribution of 0 and 1 (b) bit correlation

Figure 5.12 bit correlation test which are showing same correlation value that is 0.25. This is clear indication of a very good random number generator.

It can be noticed from figure 5.12 that the correlation has a small distribution around a mean value. In order to investigate this we plotted the histogram of the correlation values. These distribution are shown in figure 5.13 histogram bit correlation. It can be noticed that the distribution of the correlation is very narrow about their mean value.

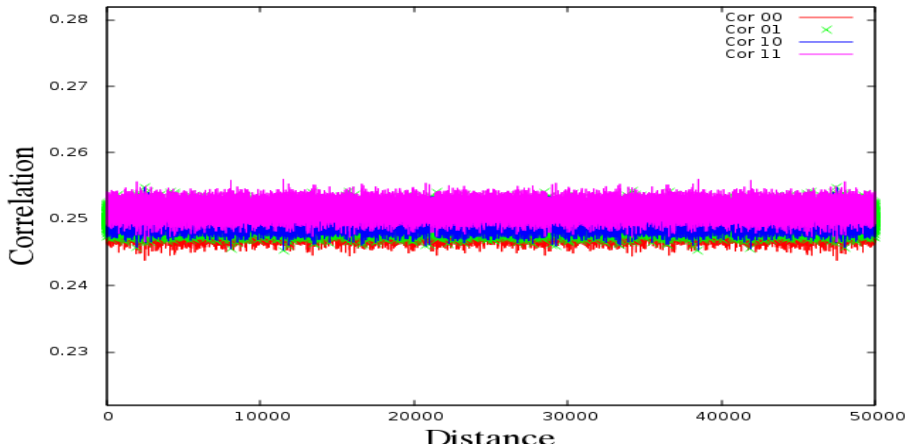


Figure 5.13: Successive bit correlation

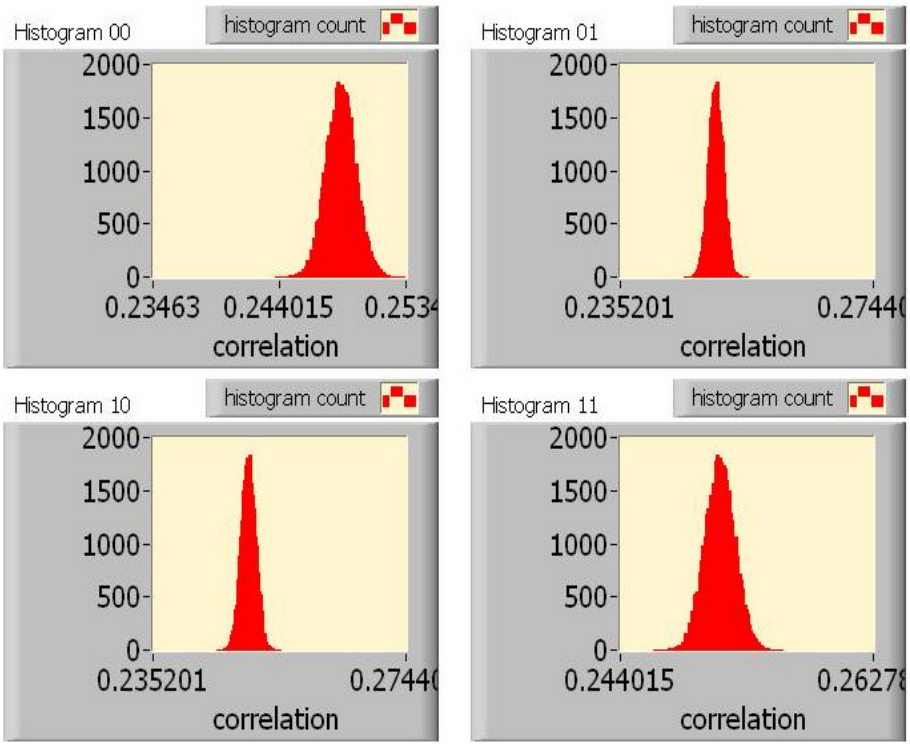


Figure 5.14: Histogram distribution probable finding pair of 00,01,10,11

NIST test

In addition to the correlation test we collected a bit stream of 0's and 1's from the circuit and process through NIST test suite. The result are as

Statistical test	P-value
Frequency	0.739918
BlockFrequency	0.350485
CumulativeSums	0.534146
CumulativeSums	0.534146
Runs	0.911413
LongestRun	0.739918
Rank	0
FFT	0.066882
NonOverlappingTemplate	0.122325
NonOverlappingTemplate	0.035174
NonOverlappingTemplate	0.213309
NonOverlappingTemplate	0.066882
NonOverlappingTemplate	0.066882
NonOverlappingTemplate	0.000954
NonOverlappingTemplate	0.004301
NonOverlappingTemplate	0.017912

Table 5.3: Result for P-value and passing sequence
In table 5.3 p-value shows more than 0.5. It means its a good random that we can use for encryption.

5.8 Conclusion

Since software methods only offer a pseudo random number codes, need for other sources is important. We have therefore analyzed a few method of generating random number. In this chapter we studied three different methods for producing random number. We have tested the out put by studying its frequency, correlation as well as the test suit from NIST. Although the correlation test gives very good result, the NIST test suite shows that some of them pass through.

Bibliography

[1] C.H. Bennett and G. Brassard In: Proc. IEEE Int. Conf. on Com- puters, Systems, and Signal Processing at Bangalore, IEEE, New York , p.

175.1984

[2] Security requirements for cryptographic modules. FIPS 1402 (2001). http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[3] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, Theory of spread-spectrum communications-a tutorial, IEEE Trans. Commun. 30(5), 855884, 1982

[4] N. Metropolis and S. Ulam, The Monte Carlo method, J. Am. Stat. Assoc. 44(247), 335341,1949

[5] M. Nazarathy, S. A. Newton, R. P. Giffard, D. S. Moberly, F. Sischka, W. R. Trutna, Jr., and S. Foster, Realtime long range complementary correlation optical time domain reflectometer, J. Lightwave Technol. 7(1), 2438, 1989

[6] C. Petrie and J. Connelly, A noise-based IC random number generator for applications in cryptography, IEEE Trans. Circ. Syst. I Fundam. Theory Appl. 47(5), 615621, 2000

[7] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC, IEEE Trans. Comput. 52(4), 403409, 2003

[8] T. Stojanovski and L. Kocarev, Chaos-based random number generators-Part I: analysis, IEEE Trans. Circ. Syst. I Fundam. Theory Appl. 48(3), 281288, 2001

[9] T. Stojanovski, J. Pihl, and L. Kocarev, Chaos-based random number generators-Part II: Practical realization, IEEE Trans. Circ. Syst. I Fundam. Theory Appl. 48(3), 382385, 2001

[10] John Callas, Using and Creating Cryptographic-Quality Random Numbers, http://www.merrymeet.com/jon/usingrandom.html, 3 June 1996

[11] Tim Matthews,Suggestions for random number generation in software, RSA Data Security Engineering Report, 15 December 1995 (reprinted in RSA LaboratoriesBulletin No.1,22 January 1996).

[12] Cryptographic Random Numbers, IEEE P1363 Working Draft, Appendix G, 6 February 1997

[13] Zufallstreffer, Klaus Schmeh and Dr.Hubert Uebelacker,"Cryptographic Security Architecture: Design and Verification", No.14, 1997

[14] Donald Knuth, Addison-Wesley, The Art of Computer Programming: Volume 2, Seminumerical Algorithms, 1981

[15] Alfred Menezes, Paul van Oorschot, and Scott Vanstone Handbook of Applied Cryptography, CRC Press, 1996

[16] Oded Goldreich Foundations of Cryptography Fragments of a Book, February 1995

[17] http://www.stat.fsu.edu/pub/diehard/

[18] Helen Gustafson, et. al., "A computer package for measuring the strength of encryption algorithms," Computers & Security, Volume 13, pp. 687-697, 1994.

[19] Andrew Rukhin, Juan Soto, James Nechvatal,"A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications"NIST Special Publication 800-22

[20] G. Marsaglia, DIEHARD Statistical Tests: http://www.stat.fsu.edu/pub/diehard/.

[21] I. J. Good, The serial test for sampling numbers and other tests for randomness, Proc. Cambridge Philos. Soc. 47, pp. 276-284,1953

[22] M. Baron and A. L. Rukhin, Distribution of the Number of Visits For a Random Walk, Communications in Statistics: Stochastic Models. Vol. 15, pp. 593-597,1999

[23] Frank Spitzer, "Principles of Random Walk", Princeton: Van Nostrand, especially p. 269,1964

[24] T. Kuusela "Random Number Generation Using a Chaotic Circuit"J. Nonlinear Sci. Vol. 3: pp. 445-458, 1993

[25] Paul S. Linsay,"Period Doubling and Chaotic Behavior in a Driven Anharmonic Oscillator" phy rev lett, 1981

Chapter 6

LabVIEW Programming for PolSK

6.1 Introduction

In this chapter we discuss the design and implementation of protocol for PolSK using labVIEW (Laboratory Virtual Instrumentation Engineering Workbench)[1, 2, 3]. In order to make the communication networks between two nodes we must establish communication interface between them, including hardware and software parts. The interface hardware part achieves physical connection and information transfer between nodes. The software part implements a communication protocol.

Virtual instrument development tools LabVIEW is a graphical programming language that easy to read and understand [4, 5]. LabVIEW has two basic windows, front panel and rear panel. Front panel is an interactive windows that displays input and output of program and Program running results can be seen on the front panel. Rear panel is the graphical source code window, and each input and output controls in front panel has its corresponding icon in rear panel. How the results in front panel are achieved in the rear panel is easily seen. Otherwise, the same as manipulate traditional instruments with their

hands, we can manipulate the virtual instrument with mouse. With help of LabVIEW from logic blocks and other components, makes it possible to test, simulate and control flowchart type model [6]. LabVIEW consist of readily available modules for interface of external hardware. This aspect of labVIEW is most useful for other application. Arrange of different connectivity such as DAQ card, IEEE GPIB, serial port etc are allowed by labVIEW through easily configurable modules. In particular we make use of multi-function DAQ cards for both transmitter as well as receiver modules. More detail for the same are providing in coming sections. Lab VIEW is an ideal tool for CAI(computer assisted instruction)[7].

The LabVIEW which represents the graphical development environment is not only powerful, but also can effectively reduce the cost of development applications [15]. With the development of network technology and applications, Achieving network applications, which is based on the virtual instrument technology based on the LabVIEW is a researched focus in the current domestic [16, 17, 18]. Hardware devices use data acquisition card and interface board. The LabVIEW platform realized data acquisition and data transmission [19, 20, 21]. LabVIEW can be connected to different PLCs (Programmable Logical Controllers) via different industrial communication protocols, for example through Ethernet, Profibus, ProfiNET protocols. It can be implemented into process controls ranging from small scale to large scales. It is easily integrated with hardware devices such as the FPGA[22, 23]. Except the fact that a graphical programming language is more user-friendly, the LabVIEW software has benefits considering the following two big differences from other programming languages [24]

- Graphical programming is realized with help from graphical icons, combined in a diagram and is then directly compiled to machine code, so that the processor can understand and execute the orders created in the diagram.

- Data flow is transmitted in form of data (not lines of text). This makes it

easier to control different executions done separately and consecutively.

One advantage of programming in LabVIEW is that we don't have the overhead to write huge codes. Only function of the different blocks needs to be known. Additionally the other advantage is that it works on Data flow Programming principle, i.e. the output is only obtained when all the inputs get their input data. Using its signal processing functions and scope chart, we can observe the treatment results of before and after signal processing in the form of time-domain waveform or frequency-domain spectrum chart.

6.2 PolSK free space communication based on labVIEW

We have earliear explain about PolSK and shown its experimental setup. To begin according experimental set we must have establish software parts. In the Software part we are going to discuss about the Authentication and handshaking protocols which are the basis for any communication protocol and the error correction codes and how to do privacy amplification. Any communication protocol consists of these parts

- Authentication
- Handshaking
- Data transfer
- Error correction and
- Privacy amplification

A simple program would have components as given by the diagram figure 6.1. The figure 6.1 is showing the communication protocol. The component of theis protocol is as follows.

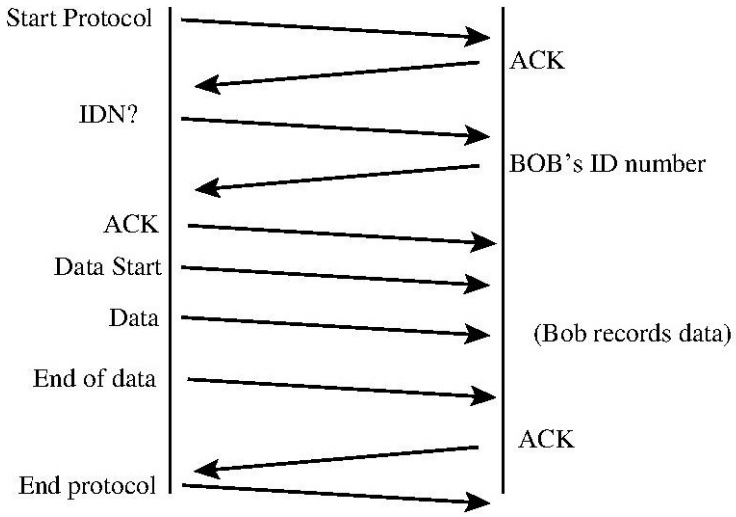


Figure 6.1: Schematic diagram for optical communication protocol

- Alice initiates the protocol, by the "start protocol" command.
- Bob acknowledge receipt of the command.
- Alice ask Bob to identify himself. Bob identifies with a pre approved ID code. If this is the same as the pre-saved code with Alice, then Alice confirms the ID. This is to prevent any unauthorized communication. This also prevents an eavesdropper posing an authorized receiver.
- Once Bob's authentication is approved Alice initiates data transfer with a "Data start"command. Bob starts saving the received data on this command.
- Alice concludes the data stream by end of data command. Bob stops recording the data. Bob acknowledges by ACK command.
- Alice completes the protocol by End protocol.

We have implemented this entre operation using labVIEW. We divided this protocol in transmitter and receiver portion so that programs can be written for each part. To integrate this protocol onto hardware we use two data acquistion

cards or DAQ cards PCI 6320 and PCI 6325. Both have a acquisition data of 250 kS/s, 24 digital I/O lines, 1MHz maximum digital I/O rate with digital triggering and composed of analog output, digital I/O and counters. for the transmitter case we have used PCI 6325 for receiver case the TTL pulses corresponding to APD output to the counter of ctr0 and ctr1. The protocol was implemented on a hp Intel[R] Core 2Duo CPU, E8400 @ 3.00GHz , 2.99GHz, 2.97GB of RAM. LabVIEW for Windows Microsoft XP, Professional was used with package National Instruments LabVIEW 8.2.1 installed.

6.2.1 LabVIEW transmitter

For the transmitter part, we use the digital I/O of the DAQ card PCI-6325. The TTL output from these pins are fed to a voltage differentiatior, which in terms generats a pulse of 0.7 V for every TTL output of the PCI-6325. This 0.7 V output is fed to the the Thorlabs VCSEL controller VITC002, which switch on the VCSEL beyond its threshold value. The remaining setup is as explained in chapter 2. The figure 6.2 is flow chart for transmitter and corresponding labVIEW program written in figure 6.3 and figure 6.4.

To write this program we use all functions >> measurement I/O >>NI DAQmx>>write. We can configure according to require signal digital or analog. We have chosen port0 to transfer digital signal. In figure 6.3 rear panel of transmitter which creates random bits and write to pors. Figure 6.4 for receiving authentication protocol. Corresponding front panel can seen in figure 6.5.

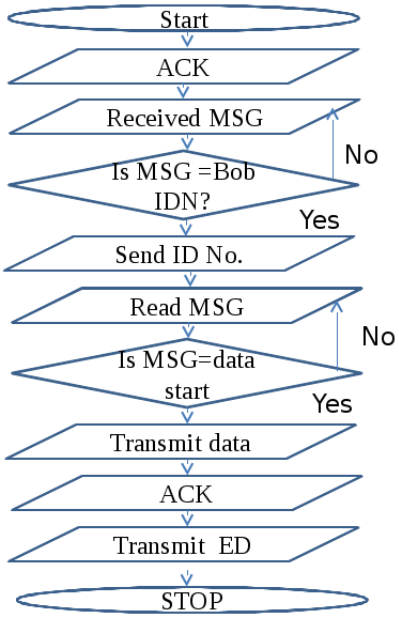


Figure 6.2: Flow chart diagram for transmitter

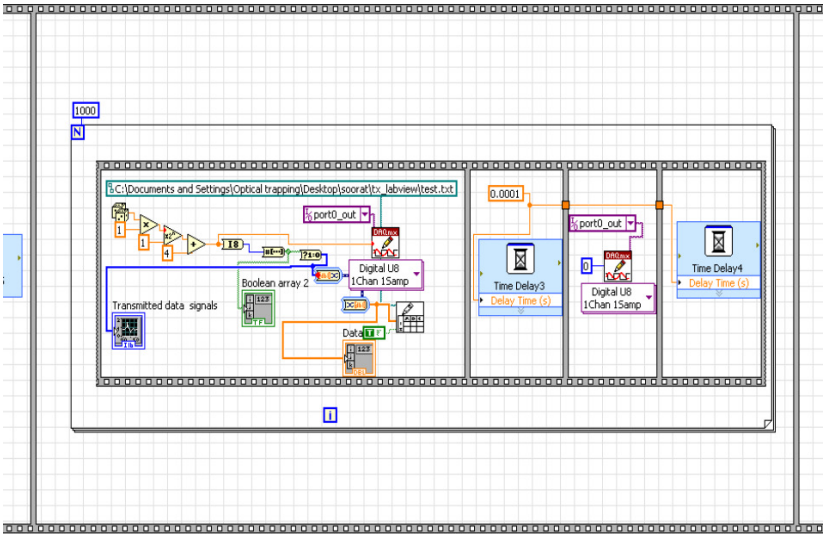


Figure 6.3: Rear panel of transmitter which creates random bits and write to port0

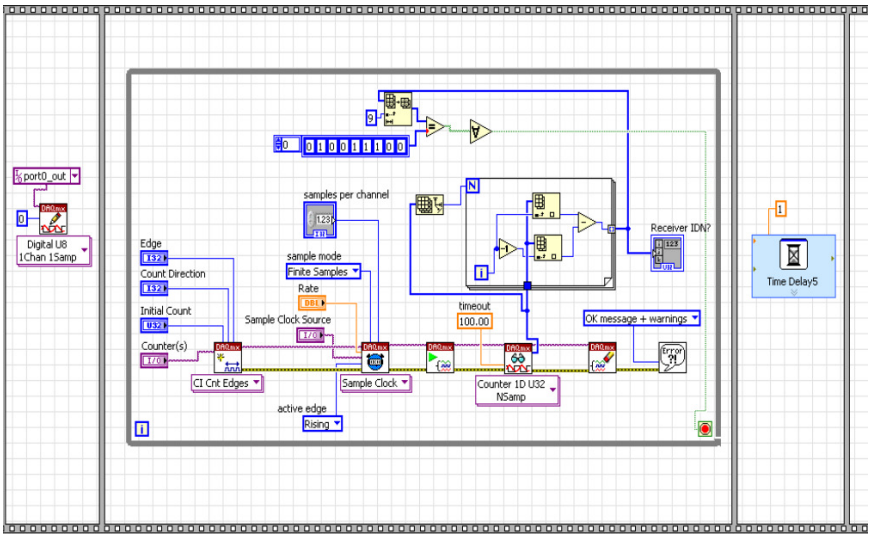


Figure 6.4: Rear panel of Alice for receiving authentication protocol

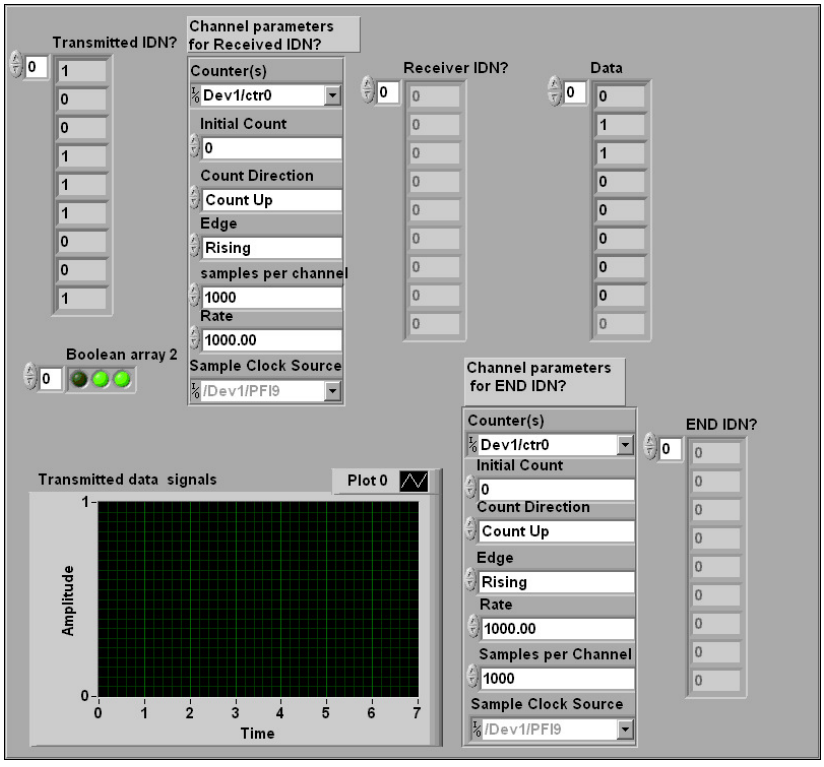


Figure 6.5: Front panel of transmitter

6.2.2 LabVIEW receiver

For the receiver, the TTL pulses from the SensL module are connected to the counter input of PCI-6320. The figure 6.6 is flow chart for receiver and corresponding labVIEW program written in figure 6.3.

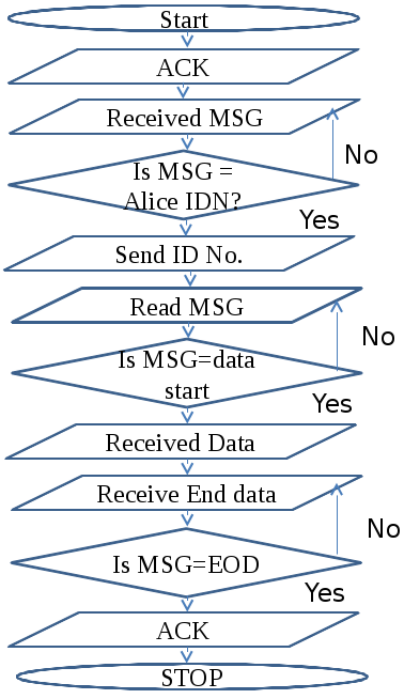


Figure 6.6: Flow chart diagram for receiver

This program shows how to count a finite number of buffered digital events on a counter input channel figure 6.7. As explained earlier, the TTL output from the APD's are connected to the two counter input of PCI 6320. However the corresponding labVIEW module will only give total counts. We need it to count the number of pulses within the period of the synchronizing pulse. We run our program up to 5 kHz and counted 2.5 KS/s.

Block Diagram Steps are as follows

- Create a Counter Input channel to Count Events. The Edge parameter is used to determine if the counter will increment on rising or falling

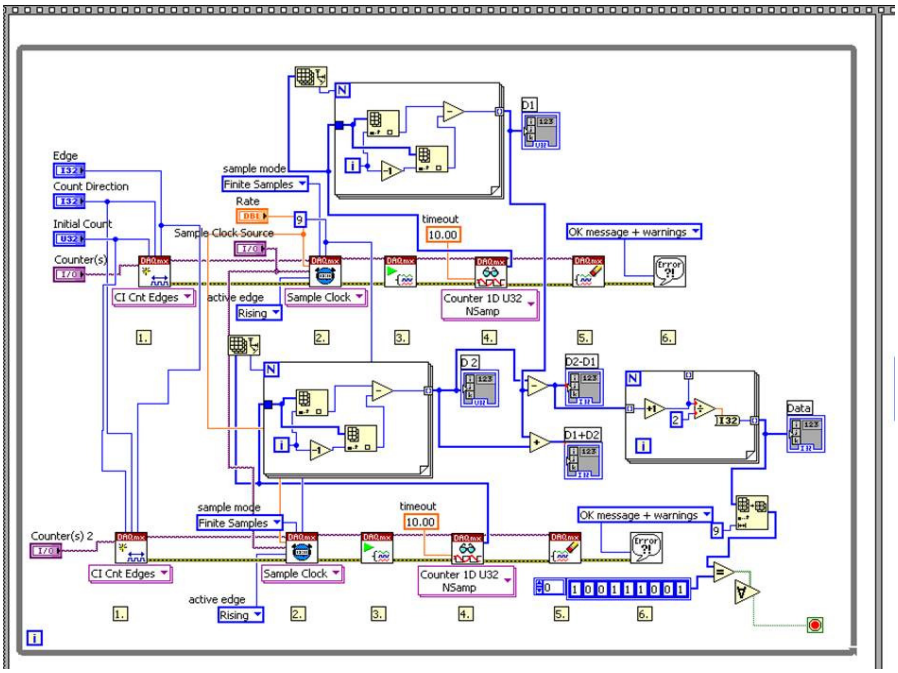


Figure 6.7: Rear panel of receiver

edges.

- Call the DAQmx Timing VI (Sample Clock) to configure the external sample clock timing parameters such as Sample Mode, Samples per Channel, and Sample Clock Source. The Edge parameter can be used to determine when a sample is taken.
- Call the Start VI to arm the counter and begin counting. The counter will be preloaded with the Initial Count.
- For finite measurements, the counter will stop reading data when the Samples per Channel have been received.
- Call the Clear Task VI to clear the Task.
- Use the pop-up dialog box to display an error if any.

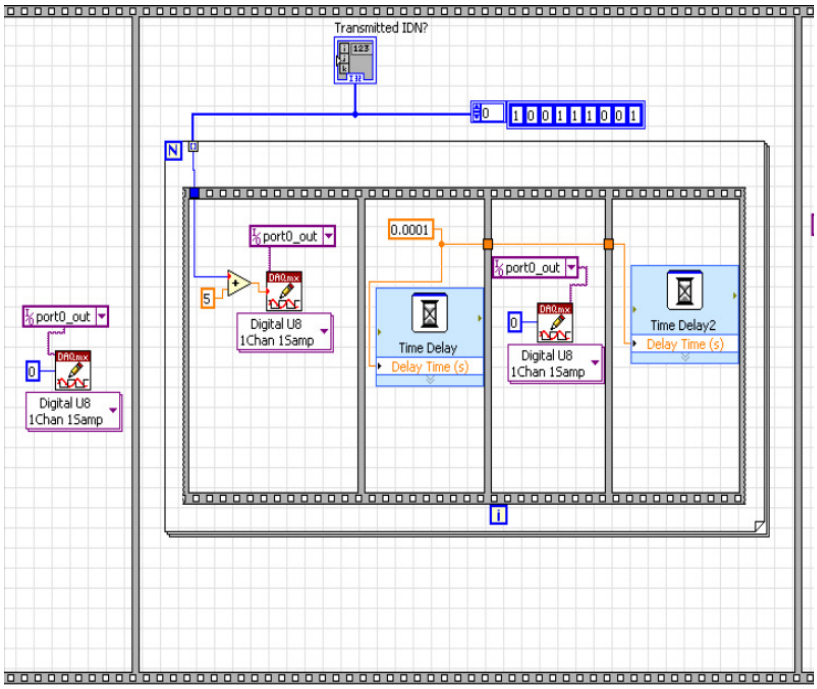


Figure 6.8: Rear panel of Bob for authentication protocol

The counter will count edges on the input terminal of the counter specified in the Physical Channel I/O control. In this program the counter will count edges on the specified input terminal on ctr0 and ctr1 from APD_1 and APD_2. The counter will take measurements on valid edges of the external Sample Clock Source which is PFI9 in this program. The oputput of counter signal we converted in to 0's and 1 based on $SoP = \frac{APD_1 - APD_2}{APD_1 + APD_2}$ values. If Sop is positive means 1 or 0 if SoP is negative. Corresponding front panel of receiver shows in figure 6.9.

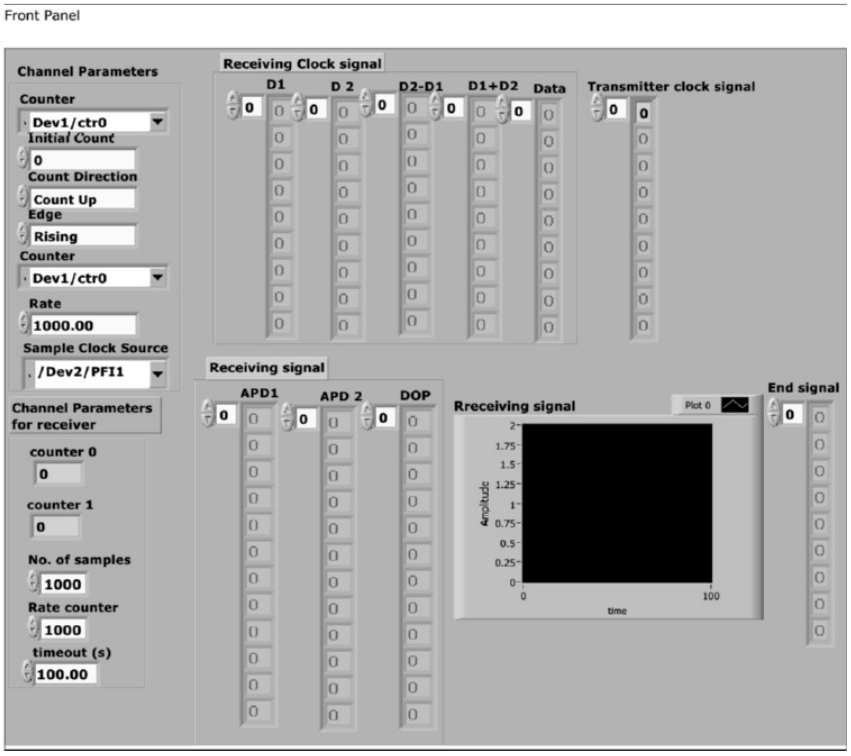


Figure 6.9: Front panel of receiver

6.3 Error correction

Error-correcting codes provide a mathematical method of not only detecting these errors, but also correcting them. Nowadays error correcting codes are ubiquitous; they are used, for example, in cell-phone transmissions and satellite links, used extensively in storage systems like compact disk and so on. There are several types of error correction codes are.

- Binary repetition code (used to for decision making Yes or No)
- Binary parity check code(used to check the presence of error for large data)
- Hamming code (used to correct single error in a block of data)
- Read Solomon code(used for burst errors like a scratch on CD)

Hamming code is best suited to correct transmission errors, we incorporated a (7,4) Hamming code within our protocol. Details of a typical hamming code are as given below.

Information Rate of a code : The ratio $\frac{k}{n}$ defines the information rate of a code

k : The number of message bits in each code word.

r : The number of check bits in each code word.

n : The block length of the code. n = k + r

For [7,4] hamming code the rate of the code is 4/7, so that for every four information , there are three check symbols introduced which are called parity check symbols.

6.4 7,4 Hamming code

When data send over a communication channel due to turbulence noise occurs. An $[n, k, d]_q$ classical linear Error Correcting Code (ECC) C is an encoding that maps k q-ary information symbols into q-ary code words of length n. The minimum distance d is the minimum number of positions where two code words differ. The encoding is completely described by an n k matrix G, called the generator matrix. Equivalently, the code is defined by the parity check matrix H, which is the (n k) k matrix satisfying HG = 0. The dual of a code C, denoted by C , is generated by the check matrix of C. Several bounds are known for the parameters of these codes, such as the Gilbert-Varshamov bound and the Hamming bound [26].

A classical $[n, k, d]_q$ linear ECC satisfies the Singleton bound, given by

$$d1 \lesssim nk$$

Codes that satisfy the Singleton bound with equality are called Maximum Distance Separable (MDS) codes. These codes have some special properties. Note that a q-ary code is systematic on a set of k coordinates, if every of the qk

possible combinations on those k coordinates occurs exactly once.
Given an [n, k, d] classical code C. Then the following statements are equivalent.

- C is an MDS code.
- C is systematic on any k coordinate positions.
- If [I—G] is the generator matrix for C, then every square submatrix of G is nonsingular.
- The dual code of C is also an MDS code.

The mathematics of 7,4 Hamming code can be explained as follows.
Let data bits be d_1, d_2, d_3, d_4 and the parity bits p_1, p_2, p_3. such that

$$p_1 = d_1 \oplus d_2 \oplus d_4$$

$$p_2 = d_1 \oplus d_3 \oplus d_4$$

$$p_3 = d_2 \oplus d_3 \oplus d_4$$

The arrangement of all data is given as

$$p_1, p_2, d_1, p_3, d_2, d_3, d_4$$

This can be achieved by a Generator matrix G operating on data matrix D as

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = P \tag{6.1}$$

P is the parity matrix

$$\textit{The parity check matrix } H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Operating H on P gives "Syndrome vector". This HP gives three bit vector.

$$HP = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ d_1 \\ p_3 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix}$$

$$\begin{pmatrix} p_1 \oplus d_1 \oplus d_2 \oplus d_4 \\ p_2 \oplus d_1 \oplus d_3 \oplus d_4 \\ p_3 \oplus d_2 \oplus d_3 \oplus d_4 \end{pmatrix} = \begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \end{pmatrix} = Z \tag{6.2}$$

Alice transmits d_1, d_2, d_3, d_4 as well as p_1, p_2, p_3 that is the complete P vector Bob computes Z as per above formula 6.2 if all Z_1, Z_2, Z_3 are zero there is no error. else the position of error come to found from the value of Z.

Due to intentional arrangement of order of p, we knows that if lets say d_1 has flipped then

$$Z = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = 011 = 3$$

based on that be can say 3 bit got flipped same way if d_2 flipped

$$Z = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = 101 = 5$$

similarly if d_3 flipped bit number is 6^th for d_4 bit number is 7. These bit can be corrected.

6.4.1 Implementing Hamming using LabVIEW

Suppose that Alice and Bob each have a bit string that can be divided in to subsets of 7 bits and that suppose they are confident that their strings differ in at most one place in 7,they will go for Hamming code which can correct 1 bit error in every 7 bits ([7,4] hamming). We have built a LabVIEW program for

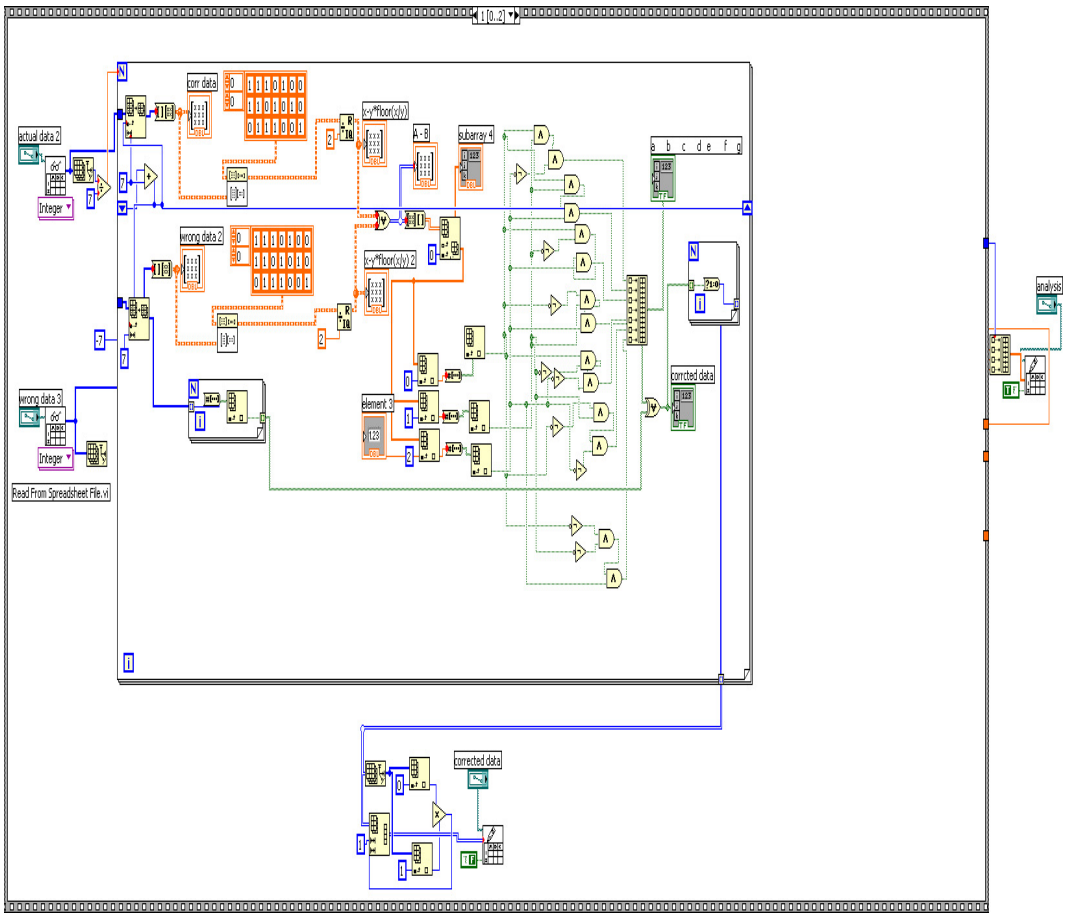


Figure 6.10: Hamming error correction program

Hamming error correction. figure 6.10shows hamming error correction code

program. To check the efficiency of the hamming code, we have generated random bits which are multiple of 7 (7-35000 bits) and we have introduced error from 0 % to 20% of the total number of bits then we have implemented hamming on them. Then checked how many number of bits are equal to the correct bits then plotted a graph between before hamming code and after hamming code. In this case transmitter transmit all the data bits and transmit the parity bits afterwards. This is different from the standard practice of a bit string with parity embedded in data bits as explain in previous section.

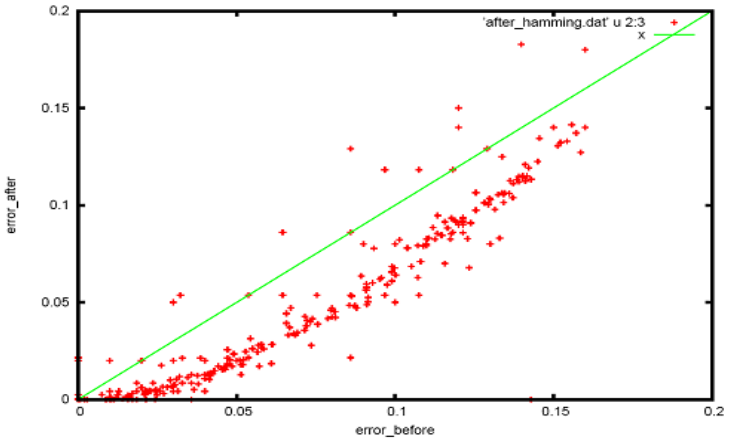


Figure 6.11: Efficiency of Haming code in correcting Bob's information. Graph shows error rate after Hamming operation v/s initial error rate. Straight line represents no change in error rate (i.e., no Hamming). Hamming operation decreases the error rate.

Green line indicates x=y i.e after hamming is equal to before hamming we can see the red line is almost every time below the green except for few cases this is because of some burst errors (i.e if more then 1 error occurs)

While Hamming code is effective in correcting transmission errors, it creates additional problems in cryptography applications. This is because any eavesdropper may have access to syndrome set. In an extension of our work to quantum key distribution, which is explained in chapter 6, we reworked our protocol to transmit the data in quantum channel, while the parity bits are separates. In such case, eavesdropper has access to the parity bits. While eve's measurement of quantum bits leaves a footprint and her presence can be thus detected, the parity bits are on public channel.

We simulated a situation where in Eve uses these parity bits to correct her information as well. However, since Eve does not attempt to measure all the bits transmitted, she will have incomplete information. Her information contents depends upon the number of bits measured by her.

If we assume that Eve measures n number bits and pads the remaining bits by guessing their value, will she be able to improve he knowledge using

the parity bits? We tested this question in our simulation. Our simulation program randomly picks up data bits from Alice's bit-stream and inserts the m at same places in Eve's data. Remaining bits of Eve's data are randomly put by the program as 0 or 1. After this Alice and Bob compare their basis sets ad creates a shifted key. After this Alice computes the parity of the shifted key sequence and shares equally with Bob's program as well as Eve,s program. Both Bob and Eve program use this parity sets on their respective data bits. The result of this exercise on a about 50 different data sets are shown in figure 6.12.

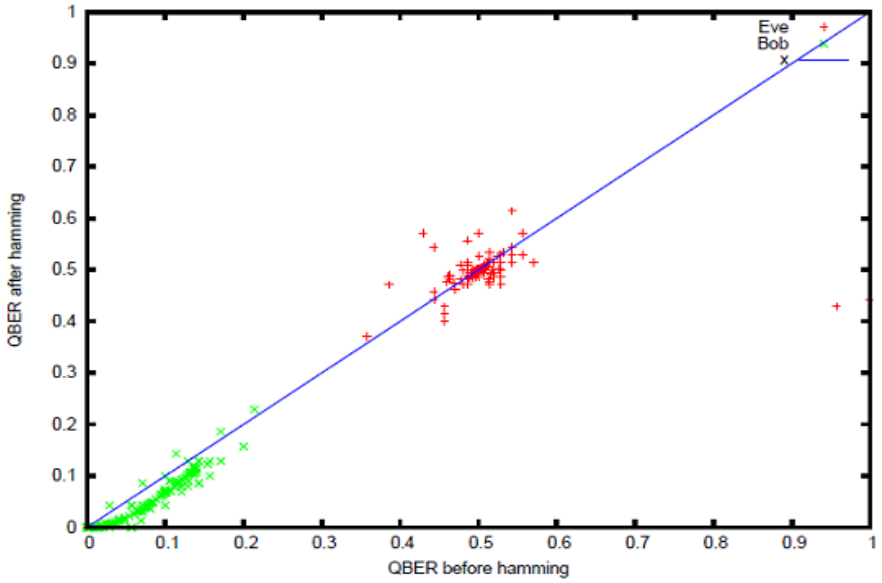


Figure 6.12: Bobs Generator matrix operated on Eves information as well. Compared with Bobs error rate on same graph. Bobs error rate decreases after Hamming, but Eves remains same.

QBER is calculated for both Bob and Eve before and after hamming. Hear blue line indicates x=y, we can clearly see that hamming is not helping eve much as before hamming and after hamming the QBER for Eve is almost the same.

To calculate the error rate after Hammming we have plotted the error rate of Eve and Bob after hamming with respect the Eves measurement(i.e the percentage of errors introduced) in figure 6.13

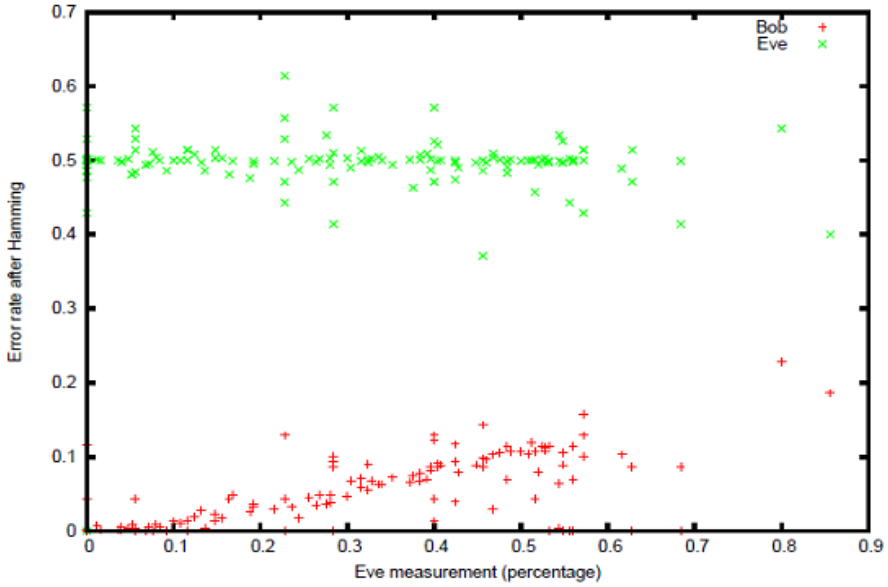


Figure 6.13: QBER after Hamming as a function of Eves measurements. Hamming is effective (for Bob) when Eves measurement is small. However, Eves error rate is same for all measurements.

6.5 Conclusions

In this chapter we explain a complete program for standard requirement of a traditional protocol such as hand shaking, identification and acknowledgment. We also created a LabVIEW code for error correction of the data using (7,4) hamming code. It was tested by deliberately causing known rate of bit flip errors on a test data. The data after operating Hamming correction was compared with the original data and the uncorrected bit error rate was obtained. We found that bit error rate after hamming code correction is much smaller.

Bibliography

[1] Xuan Weng, Xinyuan Zhao "An Experiment of Polarization Measurement Using DSP-based Control System", Proc. of SPIE-OSA-IEEE/ Vol. 7630 76300H-1, 2009

[2] Ye Yu, Yangan Zhang, Xueguang Yuan "A LabVIEW-based real-time measurement 38 system for polarization detection and calibration"Optik, 2014

[3] Joon-ho Choi Eun-byeol Cho "Visible light communications employing PPM and PWM formats for simultaneous data transmission and dimming"Opt Quant Electron DOI 10.1007/s11082-014-9932-0, 2014

[4] RenBo, Li Huan "A Communication Platform for Teaching Based on LabVIEW"2010 International Conference on Educational and Network Technology (ICENT), 2010

[5] LIU Yitong, SHI Lei "A Virtual Telephone Communication System Based On LabVIEW"ICALIP, 978-1-4244-5858-5/10, 2010

[6] Jeffery Travis, Jim Kring, LabVIEW for Everyone- Graphical programming made easy and fun 3rd edition, Prentice Hall, 2007

[7] Yi Wu, Ruixia Yang. "LabVIEW-based digital circuit simulation," Control and Automation Publication Group, 2007

[8] Tiecheng Song, "Communication Theory teaching practice," Journal of Electrical and Electronic Education, 25 (5), 95-97, 2003

[9] Wenxin Chen, Weidong Chen, "Communication Theory multi-faceted reform and practice,"Journal of Ningbo University of Technology, 19(4):88-90, 2007

[10] Shibing Zhang, Guoan Zhang. "Communication Theory Teaching Reform and Practice, "Journal of Electrical and Electronic Education, 28 (4): 10-13, 2006

[11] Rick Bitter, Taqi Mohiuddin, Matt Nawrock. LabVIEW Avanced Programming Techniques, 2nd Eddition, Motorola, Taylor & France Group, 491:13: 0 8493 3325 5, 2007

[12] NI Eductional Laboratory Virtual Instrumentation Suite II (NI ELVIS II) User Manual, National Instrument Corporation, 33: 374629A-01. April 2008

[13] Jiafu Zhu,"The Virtual Technology in Electronic Information Course Teaching,"Journal of Western Chongqing University(Social Sciences), 27 (3) :88-90, 2008

[14] Chao Chen. "MATLAB simulation experiment in communication theory courses teaching," Experimental Technology and Management, 24 (5),92-93,2007

[15] YANG Le-ping, LI Hai-tao, ZHAO Yong," High-level LabVIEW programing Design" Beijing,Tshing Hua University Publishing House,2003

[16] F J, Jime nez, J,De Frutos, " Virtual instrument for measurement,processing data, and visualization of vibration patterns of piezoelectric devices" Computer Standards and Interfaces, pp. 213216, 2005

[17] Li Ren-fa, Network Architecture of Virtual Lab[J], Acta Simulata Systematica Sinica, 14 (3), pp. 359362, 2002

[18] NIE Chun-yan, "An application of virtual instrument in laboratory",Journal Changchun University, 2004

[19] MURATBY EREFZST "Design and implementation of labVIEW based data acquisition and image reconstruction enviorment for METU-MRI" middle east technical university, 2005

[20] HANS PETTER H ALVORSEN "Data Acquisition in LabVIEW" 2013

[21] Weilin Wang a, Changying Li "Development of software for spectral imaging data acquisition using LabVIEW"Computers and Electronics in Agriculture, 2012

[22] Carrie L. Saunders, "LabVIEW software development for input and output mesurement and control of FLEX lab" Russ College of Engineering and Technology of Ohio University,2006

[23] F. Ziegler , D. Beck "A new Pulse-Pattern Generator based on LabVIEW FPGA"Nuclear Instruments and Methods in Physics Research A 679,2012

[24] Harjot Singh Saini "A labVIEW based power converter design for time domain electromagnetic system", Concordia University Montreal, Quebec, Canada.

[25] G. W. JOHNSON, LabVIEW Graphical Programming, McGraw-Hill, 1994.

[26] K. P. T. Riejens, Master's thesis, Eindhoven University - unpublished.

Chapter 7

Conclusion & Future work

7.1 Conclusions

In this thesis we have examined the key issue of noise due to atmospheric effect in free space PolSK scheme. polarization scrambling due to fog and smoke is a serious issue in case of free space PolSK schemes. However, we have shown a differential measurement method which picks out the snake and ballistic photons and gives a reliable state of polarization, even in presence of a large depolarization noise. This indicates that polSK is a robust and practical scheme despite the initial indication otherwise.

After a brief overview of the fundamentals of FSO in the first two chapters, we present our method in chapter 3. We simulate atmospheric condition such as smoke and fog in a glass chamber in the path of beam. Despite a large degree of depolarization due to multiply scattering by fog of smoke particle, the information can still be extracted. This is due to the proposed method of differential polarization which overcomes the noise. In addition this is also simpler, since it involves only two measurement as against six measurement

required for full stokes vector characterization.

In chapter 4 we showed that the noise pattern is different for 45°/135° polarization. This information has relevance for m-ary encoding as well as our future ideas of QKD. Random numbers are an important part of any cryptographic scheme. It is also important to test communication scheme. We tested and reported three different methods of generating random numbers. We tested the output against NIST test suite.

We reported a full labVIEW program that takes care of the complete protocol for communication including authentication, handshaking and error correction. A 7,4 Hamming code is built in to the labVIEW program. We also showed tht this Hamming code improves the signal of authenticated receiver,but can not help any eavesdropper, as long as eavesdropper's information is limited. We proposed to use these data for our proposed future proposals.

7.2 Future work: Development of a prototype for free space Quantum Key Distribution(QKD)

Whenever sensitive information has to be exchanged between two parties, cryptography is employed to ensure that no unauthorized third party can get access to the content. Cryptography is the study of secret (crypto) writing (graphy). Cryptography is the art of encoding and decoding messages and has existed as long as people have distrusted each other and sought forms of secure communication [1, 2]. Although the field of cryptography is ancient, it is not static. Cryptographic techniques have evolved over the centuries, with the code-makers working to stay ahead of the code-breakers . Cryptography is a technique to assure some parties to communicate over an open channel in a secure way. Classical cryptographic methods like the one-time pad have been shown to be provably secure, if and only if the key has been deployed securely. Yet, this task cannot be provably accomplished by classical means. Classical Cryptography, the history of which has at least 4000 years as we know [3],

is mainly used in diplomacy and war over centuries. However, comparing to modern cryptography which are mainly used in computer security nowadays, most of the classical ciphers are claimed to be vulnerable in front of todays powerful computers. The security of most cryptosystems is based on the assumption of computational complexity, which is strongly challenged by the increasing capability of computation or algorithms differently.

Quantum cryptography, also known as quantum key distribution (QKD), takes advantage of the unique and unusual behavior of microscopic objects to enable users to securely develop secret keys as well as to detect eavesdropping [4, 5, 6, 7, 8, 9]. QKD makes use of fundamental principles of quantum mechanics to ensure the security of secret key generation. Although work on quantum cryptography was begun by Stephen J. Wiesner in the late 1960s, the first protocol for sending a private key using quantum techniques was not published until 1984 by Bennett and Brassard. The development of quantum cryptography was motivated by the short-comings of classical cryptographic methods, which can be classified as either public-key or secret-key methods. Public-key encryption is based on the idea of a safe with two keys: a public key to lock the safe and a private key to open it. Using this method, anyone can send a message since the public key is used to encrypt messages, but only someone with the private key can decrypt the messages. Since the encrypting and decrypting keys are different, it is not necessary to securely distribute a key. The security of public-key encryption depends on the assumed difficulty of certain mathematical operations, such as factoring extremely large prime numbers. Practical Quantum Key Distribution protocols use either fiber based communication systems or a free space communication scheme. The system subject to this report employs the so-called BB84 protocol, encoding qubits in the polarisation of faint laser pulses. Ideally, one party (Alice) prepares a sequence of single photons, their polarisations being chosen randomly from four possible non-orthogonal states (e.g. horizontal, vertical and $\pm 45^0$). She sends the photons to the second party (Bob), who analyses the polarisation of each detected photon in a randomly and independently chosen basis (e.g.

either H/V or $\pm 45^0$). Afterwards both parties compare publicly their basis choices and discard those events where they had used different bases. This process is called sifting. Due to fundamental laws of quantum mechanics, an eavesdropper (Eve) cannot determine the polarization of a single photon if the polarization states are non-orthogonal. Even worse, she will introduce errors during the polarization measurement, so that the quantum bit error rate (QBER) of the sifted key gives an upper bound on the information an eavesdropper might have gained. The QBER is calculated during the classical error correction procedure and is used to infer the shrinking ratio that is needed to make sure that the information of a potential eavesdropper on the key is negligible. The key is then hashed to this secure length during privacy amplification.

The original BB84 protocol[10], which is explained in terms of polarization, is not suitable for fiber based systems since polarization is not preserved in fibers. Hence it is modified to a phase modulation scheme [11]. On the other hand, polarization is a more reliable parameter in free space systems since phase gets randomized due to atmospheric disturbances. Even in such situations, polarization does get affected due to same disturbances and the efficiency of the scheme depends critically on the efficiency of the polarization encoding. It is particularly so when using very faint laser pulses. Therefore in order to understand the dependency between efficiency of polarization encoding and that of BB84, we have made a detailed study of Polarization Shift Keying (PolSK). This study enables us to identify error rates that arise in any general PolSK schemes and errors that are specific to our hardware system.

7.3 BB84 protocol

In 1984, Bennett and Brassard suggested the first protocol, called BB84, for establishing a secret key using quantum transmissions. This protocol uses the rectilinear and circular polarization bases for photons. The steps of the protocol are briefly explained below, using the standard convention that Alice is the sender, Bob is the receiver, and Eve is the eavesdropper.

- Alice prepares photons randomly with either rectilinear or circular polarization.
- Alice prepares the polarization of each photon and then sends it to Bob.
- Bob receives each photon and randomly measures its polarization according to the rectilinear or circular basis. He records the measurement type (basis used) and the resulting polarization measured. (It is important to remember that the polarization sent by Alice may not be the same polarization Bob finds if he does not use the same basis as Alice.
- Bob publicly tells Alice what the measurement types were, but not the results of his measurements.
- Alice publicly tells Bob which measurements were of the correct type. A correct measurement is the correct type of Bob used the same basis for measurement as Alice did for preparation.
- Alice and Bob each throw out the data from measurements that were not of the correct type, and convert the remaining data to a string of bits using a convention such as: left-circular = 0, right-circular = 1 horizontal = 0, vertical = 1

7.4 Ekert Protocol

Ekert protocol, developed by Arthur Ekert and David Mermin, worke on the same principles as BB84, except that it uses entangled photon pairs instead.

In this case

- Alice creates EPR pairs of polarized photons, keeping one particle for herself and sending the other particle of each pair to Bob.
- Alice randomly measures the polarization of each particle she kept according to the rectilinear or circular basis. She records each measurement type and the polarization measured.
- Bob randomly measures each particle he received according to the rectilinear or circular basis. He records each measurement type and the polarization measured.
- Alice and Bob tell each other which measurement types were used, and they keep the data from all particle pairs where they both chose the same measurement type.
- They convert the remaining data to a string of bits using a convention such as: left-circular = 0, right-circular = 1 horizontal = 0, vertical = 1

One important difference between the BB84 and the Ekert methods is that with BB84, the key created by Alice and Bob must be stored classically until it is used. Therefore, although the key was completely secure when it was created, its continued security over time is only as great as the security of its storage. Using the EPR method, Alice and Bob could potentially store the prepared entangled particles and then measure them and create the key just before they were going to use it, eliminating the problem of insecure storage.

7.4.1 QKD and photon statistics

A prototype is being developed in our lab for implementing BB84 [1] protocol of Quantum Key Distribution (QKD) in free space. This protocol requires single photons whose polarization states are mapped to the information bits 0 and 1 of the encryption key. In normal setup, the single photons are obtained by faint laser pulses with a mean photon number of 0.1. However, a laser being a coherent source, the photon number distribution follows a Poisson distribution, even after attenuation. This leads to an unwanted situation wherein the probability of having a single photon per pulse is same as that of having two photons per pulse, thus compromising the theoretically assured security of a BB84 scheme. To overcome this problem, we tried toexploit the nature of a diode laser operating below the threshold regime. Intuitively, one assumes that this is essentially as a thermal source, since the main source of light is amplified spontaneous emission (ASE). It has been theoretically shown that such a laser is still spatially coherent [32], but what is the photon statistics of such a source? We investigated this question by experimentally verifying the photon statistics of a diode laser operating just below the threshold as well as well above it. Unlike other lasers, diode lasers are convenient to operate it these two modes, by simply adjusting the injection current.Considering a beam of light as a stream of photons rather than as a classical wave. observation of Poissonian and super-Poissonian statistics in photo detection experiments is consistent with the classical theory of light, but not sub-Poisson statistics. Hence the observation of sub- Poissonian photon statistics constitutes direct confirmation of the photon nature of light.

Classification of light by photon statistics

We can introduce our discussion of photon statistics by considering the detection of a light beam by a photon counter as illustrated in figure The photon counter consists of a very sensitive light detector such as a avalanche photodiode (APD) connected to an electronic counter. The detector produces

short voltage pulses in response to the light beam and the counter registers the number of pulses that are emitted within a certain time interval set by the user.

the statistics are described by a Poisson distribution with photon number fluctuations that satisfy eqn $\delta n = \sqrt{n}$ In general, there are three possibilities:

- sub-Poissonian statistics: $\delta n < \sqrt{n}$ non classical light
- Poissonian statistics: $\delta n = \sqrt{n}$, coherent light
- super-Poissonian statistics: $\delta n > \sqrt{n}$, incoherent

Vcsel-780nm laser light falling on APD. Here we cutting light intensity by using neutral density filter. This is control by sensl software. VCSEL laser sub threshold operated got Gaussian and above is poissonian. In order to better understand the nature of photon statistics and to test if a laser, working below threshold will provide a non-poissonian statistics, we studied the quantitative relation between an LED, a VCSEL laser diode operating below and above threshold. We found that LED exhibits a Gaussian distribution and VCSEL shows Poissonian distribution.

Second order correlation

In general$g^{(2)}$ define as

$$g^{(2)}(\tau) = \frac{E^*(t)E^*(t+)E(t+)E(t)}{E^*(t)E^*(t+)E(t+)E(t)} \tag{7.1}$$

$$g^{(2)}(\tau) = \frac{< I(t)I(t+) >}{< I(t) >< I(t+) >} \tag{7.2}$$

Where E(t) and I(t) are the electric field and intensity of the light beam at time t. The $< >$symbols again indicate the time average computed by integrating over a long time period.
Properties of the second-order correlation function $g^{(2)}(\tau)$ for classical light.

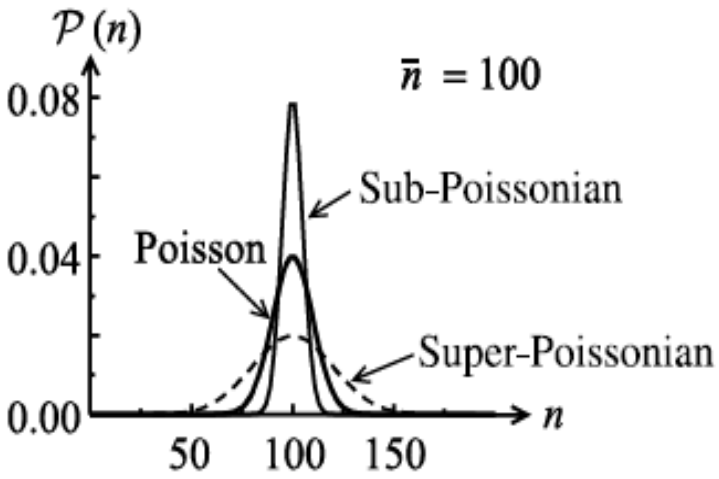


Figure 7.1: Comparison of the photon statistics for light with a Poisson distribution, and those for sub-Poissonian and super-Poissonian light. The distributions have been drawn with the same mean photon number n = 100. The discrete nature of the distributions is not apparent in this figure due to the large value of n

7.5 Experimental setup

This experimental setup figure 7.2 contains classical channel as well as quantum channel. Quantum channel (laser $L_1 to L_4$) used for key generation between users and classical channel (Laser $L_5 and L_6$) used for authentication and clock pulse. We are using Vcsel-780nm (vertical cavity surface emitting laser) for pulse generation because attenuation of 780 nm wave length light is very less in free space. Alice (transmitter) uses four lasers (laser $L_1 to L_4$)each laser is fired randomly so outcome pulses from these lasers by using polarizing beam splitter (PBS) and half wave plate is vertical, horizontal,$+45^0, -45^0$. We are using neutral density filter to make it faint pulse intensity is very low like a (single photon). This faint laser pulse is detected by Bob (receiver). We have done similer arrange for Bob so that coresponding Faint laser pulses detect by detector($D_1 to D_4$). By comparing there basis on classical channel and error correction will get secure key. If error is more than 17% then they will discard

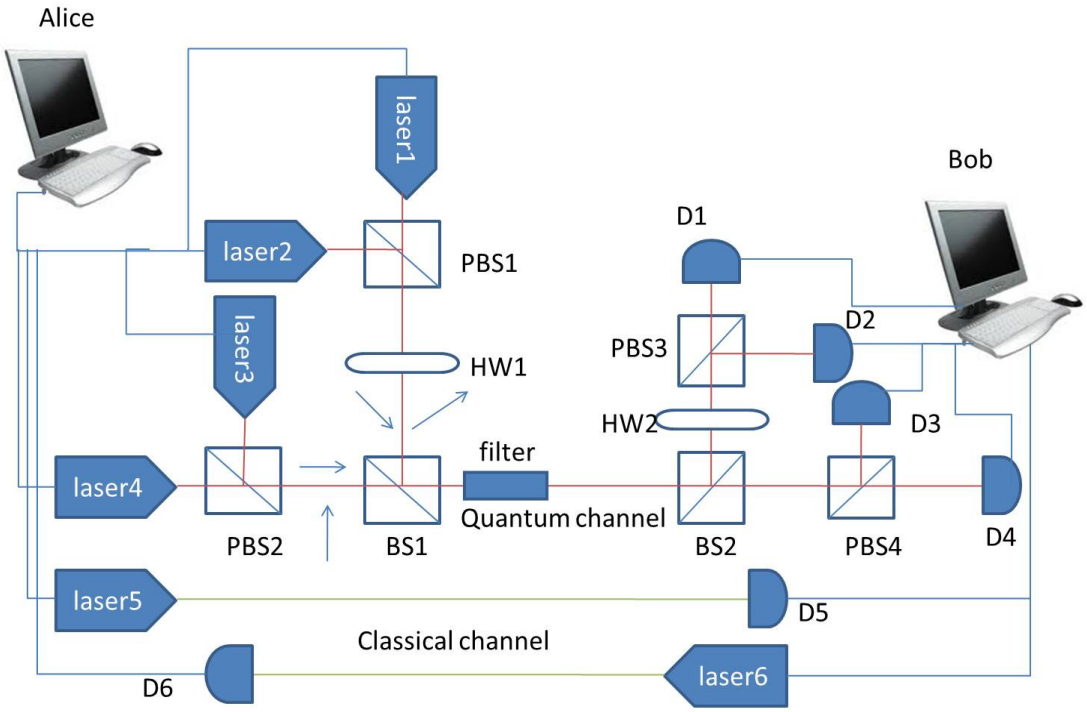


Figure 7.2: Experimental Setup

the key and they will generate fresh key. Once key establish between Alice and Bob encrypted massage send through classical channel and by decrypting this massage will give correct massage.

Bibliography

[1] Karen Hunter "quantum cryptography",SCI 510: Quantum Todd Duncan

[2] Xu Jia, Xue Ming Qiang, Zhang Weiqi, Zhu Qian"Classical Cryptography" Online:www.scribd.com/doc/36928010/Classical-Cryptographyscribd

[3] http://williamstallings.com/Extras/Security-Notes/lectures/classical.html

[4] Henning Weier, " Free space quantum key distribution:Towards a real life application"Fortschr. Phys. 54, No. 8 10, 840 845 / DOI 10.1002/prop.200610322, 2006

[5] Gerald Gilbert and Michael Hamrick "Practical Quantum Cryptography:A Comprehensive Analysis"The MITRE Corporation McLean, Virginia 22102

[6] D.N. Klyshko"Quantum cryptography using multicolored or multidirectional photons", Physics Letters A 227, 1997

[7] Valerio Scarani, Antonio Ac "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations"arxiv,feb,2004

[8] B. C. Jacobs and J. D. Franson "Quantum cryptography in free space" OPTICS LETTERS / Vol. 21, No. 22 / November 15, 1996

[9] N. Gisin et al,"Quantum cryptography" Rev. Mod. Phys. 74, 145195,2002

[10] C. H. Bennett et al. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984

[11] Christophe Marand and Paul D. Townsend Quantum key distribution over distances as long as 30 kmOptics Letters, Vol. 20, Issue 16, pp.1695-1697, 1995

List of Publications

Journal Papers

- Ram Soorat, Ashok Vudayagiri "Noise Characterization in Free Space Polarization Modulation communication Using Simulated Atmospheric Conditions in Laboratory "International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, 2014.

Under Prepration

- Ram Soorat, Ashok Vudayagiri, Noise tolerant M-ary polarization encoding in noisy atmospheric channel
- Ram Soorat, Ashok Vudayagiri, PolSK and error correction complete programming by LabVIEW
- Ram Soorat, Ashok Vudayagiri, Study of Random number Generator and its Suitable Test

Conference Papers

- Ram Soorat, Ashok Vudayagiri "Polarization Shift Keying for free space QKD: Effect of noise on reliability of the QKD Protocols", International Conference on Fiber Optics and Photonics OSA 2012"

Poster

- Ram Soorat, Ashok Vudayagiri,"Laser diode characterization for cryptography" poster at NLS-19, 1-4 Dec 2010 RRCAT Indore.
- Ram Soorat, Ashok Vudayagiri,"Laser diode and Photodiode characterization for cryptography", poster at WORKSHOP ON PHYSICS AT SMALL SCALES, 18-19 march 2011, University of Hyderabad.
- Ram Soorat, Ashok Vudayagiri, "Noise fluctuation in optical signal", poster at WORKSHOP ON PHYSICS AT SMALL SCALES, 28 October 2011, University of Hyderabad.

- Ram Soorat, Balaji Yendeti, Ashok Vudayagiri,"Study of noise correlation in polarized light using liquid crystal" poster at IONS 1-2 Dec 2011, IIT Delhi.

- Ram Soorat, "Study of noise correlation in polarized light using liquid crystal", micro talk at IONS 1-2 Dec 2011, IIT Delhi.

- Ram Soorat, Balaji Yendeti, Ashok Vudayagiri, "Polarization shift keying", poster at xxxvi OSI symposium, 3-5 Dec 2011 IIT Delhi.

- Ram Soorat, Ashok vudayagiri,"Polarization Shift Keying for free space QKD: Effect of noise on reliability of the QKD Protocols" Photonics 2012 International Conference on Fiber Optics and Photonics, Indian Institute of Technology Madras, India December 9-12, 2012.

- Ram soorat, Ashok vudayagiri,"Polarization shift keying:Towards quantum key distribution" INTERNATIONAL CONFERENCE ON QUANTUM INFORMATION AND QUANTUM COMPUTING 7-11 January 2013, IISc Banglore.

Schools attended

- Mini Winter School on Quantum Information and Computation, Indian Institute of Science, Bangalore, India, 03-05 January 2013.

- International workshop on quantum information, 20-26 feb 2012, HRI Allahabad.

- Indo-Brazil Workshop on Cold Atoms, Mesoscopic Phenomena and Quantum Information Processes, Hyderabad, India, 16-18 October 2010